SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 18 January 2023

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

Critical	vulnerabilities with a base score of 9.0 to 10.0
High	vulnerabilities with a base score of 7.0 to 8.9
Medium	vulnerabilities with a base score of 4.0 to 6.9
Low	vulnerabilities with a base score of 0.1 to 3.9
None	vulnerabilities with a base score of 0.0

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-22601	InHand Networks InRouter 302, prior to version IR302 V3.5.56, and InRouter 615, prior to version InRouter6XX-S-V2.3.0.r5542, contain vulnerability CWE-330: Use of Insufficiently Random Values. They do not properly randomize MQTT ClientID parameters. An unauthorized user could calculate this parameter and use it to gather additional information about other InHand devices managed on the same cloud platform.	10.0	More Details
CVE-2023-22600	InHand Networks InRouter 302, prior to version IR302 V3.5.56, and InRouter 615, prior to version InRouter6XX-S-V2.3.0.r5542, contain vulnerability CWE-284: Improper Access Control. They allow unauthenticated devices to subscribe to MQTT topics on the same network as the device manager. An unauthorized user who knows of an existing topic name could send and receive messages to and from that topic. This includes the ability to send GET/SET configuration commands, reboot commands, and push firmware updates.	10.0	More Details
CVE-2017-16309	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd sn_exw, at 0x9d01b3d8, the value for the `d` key is copied using `strcpy` to the buffer at `$sp+0x334`.This buffer is 100 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16304	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd sn_ex, at 0x9d01ae40, the value for the `d` key is copied using `strcpy` to the buffer at `$sp+0x334`.This buffer is 100 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16314	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_sonos, at 0x9d01c1cc, the value for the `s_speaker` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16313	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_sonos, at 0x9d01c084, the value for the `s_ddelay` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-16312	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_sonos, at 0x9d01c028, the value for the `sn_discover` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16311	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd UpdateCheck, at 0x9d01bb64, the value for the `type` key is copied using `strcpy` to the buffer at `$sp+0x270`.This buffer is 16 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16310	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_ch, at 0x9d01b7b0, the value for the `ch` key is copied using `strcpy` to the buffer at `$sp+0x334`.This buffer is 100 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16308	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd sn_exw, at 0x9d01b374, the value for the `cmd2` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16307	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd sn_exw, at 0x9d01b310, the value for the `cmd1` key is copied using `strcpy` to the buffer at `$sp+0x2d0`.This buffer is 100 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16306	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd sn_exw, at 0x9d01b2ac, the value for the `flg` key is copied using `strcpy` to the buffer at `$sp+0x280`.This buffer is 16 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16305	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd sn_exw, at 0x9d01b20c, the value for the `id` key is copied using `strcpy` to the buffer at `$sp+0x290`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16303	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd sn_ex, at 0x9d01addc, the value for the `cmd2` key is copied using `strcpy` to the buffer at `$sp+0x280`.This buffer is 16 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16316	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_sonos, at 0x9d01c898, the value for the `g_meta_page` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16302	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd sn_ex, at 0x9d01ad78, the value for the `cmd1` key is copied using `strcpy` to the buffer at `$sp+0x2d0`.This buffer is 100 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-16301	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd sn_ex, at 0x9d01ad14, the value for the `flg` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16300	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd sn_ex, at 0x9d01ac74, the value for the `id` key is copied using `strcpy` to the buffer at `$sp+0x290`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16299	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd sn_raw, at 0x9d01aad8, the value for the `d` key is copied using `strcpy` to the buffer at `$sp+0x334`.This buffer is 100 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16298	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_schd, at 0x9d01a264, the value for the `offcmd` key is copied using `strcpy` to the buffer at `$sp+0x334`.This buffer is 100 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16297	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_schd, at 0x9d01a21c, the value for the `oncmd` key is copied using `strcpy` to the buffer at `$sp+0x2d0`.This buffer is 100 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16295	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_schd, at 0x9d01a18c, the value for the `off` key is copied using `strcpy` to the buffer at `$sp+0x270`.This buffer is 16 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16294	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_schd, at 0x9d01a144, the value for the `on` key is copied using `strcpy` to the buffer at `$sp+0x290`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16315	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_sonos, at 0x9d01c3a0, the value for the `s_state` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16317	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_sonos, at 0x9d01d068, the value for the `g_group` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16292	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd g_schd, at 0x9d019c50, the value for the `grp` key is copied using `strcpy` to the buffer at `$sp+0x1b4`.This buffer is 8 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-16328	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_event_alarm, at 0x9d01eb08, the value for the `s_event_offset` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16336	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_event_var, at 0x9d01eeb0, the value for the `s_value` key is copied using `strcpy` to the buffer at `$sp+0x10`.This buffer is 244 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16335	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_event_var, at 0x9d01ee70, the value for the `s_offset` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16334	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_event, at 0x9d01edb8, the value for the `s_raw` key is copied using `strcpy` to the buffer at `$sp+0x10`.This buffer is 244 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16333	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_event, at 0x9d01ed7c, the value for the `s_offset` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16332	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_event_alarm, at 0x9d01ec34, the value for the `s_aid` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16331	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_event_alarm, at 0x9d01ebd4, the value for the `s_tid` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16330	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_event_alarm, at 0x9d01eb8c, the value for the `s_event_group` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16329	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_event_alarm, at 0x9d01eb44, the value for the `s_event_delay` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-16327	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_init_event, at 0x9d01ea88, the value for the `s_event_offset` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16318	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_sonos, at 0x9d01d16c, the value for the `g_group_off` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16326	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_sonos, at 0x9d01e5f4, the value for the `sn_sonos_cmd` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16325	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_sonos, at 0x9d01e3a8, the value for the `s_group_cmd` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16324	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_sonos, at 0x9d01e368, the value for the `s_group_vol` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16323	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_sonos, at 0x9d01e2f4, the value for the `s_group` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16322	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_sonos, at 0x9d01e228, the value for the `c_group` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16321	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_sonos, at 0x9d01e050, the value for the `s_sonos_index` key is copied using `strcpy` to the buffer at `$sp+0x1b4`.This buffer is 8 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16320	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_sonos, at 0x9d01ddd4, the value for the `s_sonos_cmd` key is copied using `strcpy` to the buffer at `$sp+0x290`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-16319	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_sonos, at 0x9d01d7a8, the value for the `g_sonos_index` key is copied using `strcpy` to the buffer at `$sp+0x1b4`.This buffer is 8 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16293	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_schd, at 0x9d01a010, the value for the `grp` key is copied using `strcpy` to the buffer at `$sp+0x280`.This buffer is 16 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16296	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_schd, at 0x9d01a1d4, the value for the `days` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16291	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_sun, at 0x9d019854, the value for the `sunset` key is copied using `strcpy` to the buffer at `$sp+0x334`.This buffer is 100 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16264	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd l_b, at 0x9d015cfc, the value for the `grp` key is copied using `strcpy` to the buffer at `$sp+0x1b4`.This buffer is 8 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16271	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd e_l, at 0x9d016c94, the value for the `as_c` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16270	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_b, at 0x9d01679c, the value for the `s_sonos_cmd` key is copied using `strcpy` to the buffer at `$sp+0x290`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16269	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_b, at 0x9d01672c, the value for the `s_speaker` key is copied using `strcpy` to the buffer at `$sp+0x2d0`.This buffer is 100 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16268	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_b, at 0x9d0165c0, the value for the `id` key is copied using `strcpy` to the buffer at `$sp+0x270`.This buffer is 16 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16267	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_b, at 0x9d016578, the value for the `val` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-16266	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_b, at 0x9d016530, the value for the `grp` key is copied using `strcpy` to the buffer at `$sp+0x1b4`.This buffer is 8 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16290	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_sun, at 0x9d01980c, the value for the `sunrise` key is copied using `strcpy` to the buffer at `$sp+0x2d0`.This buffer is 100 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16263	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd g_b, at 0x9d015a8c, the value for the `val` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16273	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd e_ml, at 0x9d016fa8, the value for the `grp` key is copied using `strcpy` to the buffer at `$sp+0x1b4`.This buffer is 8 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16262	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd g_b, at 0x9d015864, the value for the `id` key is copied using `strcpy` to the buffer at `$sp+0x290`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16260	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_auth, at 0x9d015478, the value for the `pwd` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16259	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_auth, at 0x9d015430, the value for the `usr` key is copied using `strcpy` to the buffer at `$sp+0x290`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16258	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd sn_sx, at 0x9d014f7c, the value for the `cmd4` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16257	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd sn_sx, at 0x9d014f28, the value for the `cmd3` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16256	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd sn_sx, at 0x9d014ebc, the value for the `cmd2` key is copied using `strcpy` to the buffer at `$sp+0x2d0`.This buffer is 100 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22731	Shopware is an open source commerce platform based on Symfony Framework and Vue js. In a Twig environment **without the Sandbox extension**, it is possible to refer to PHP functions in twig filters like `map`, `filter`, `sort`. This allows a template to call any global PHP function and thus execute arbitrary code. The attacker must have access to a Twig environment in order to exploit this vulnerability. This problem has been fixed with 6.4.18.1 with an override of the specified filters until the integration of the Sandbox extension has been finished. Users are advised to upgrade. Users of major versions 6.1, 6.2, and 6.3 may also receive this fix via a plugin.	9.9	More Details
CVE-2017-16272	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd e_l, at 0x9d016cf0, the value for the `grp` key is copied using `strcpy` to the buffer at `$sp+0x1b4`.This buffer is 8 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16265	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd l_bt, at 0x9d016104, the value for the `grp` key is copied using `strcpy` to the buffer at `$sp+0x1b4`.This buffer is 8 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16274	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd e_u, at 0x9d017364, the value for the `grp` key is copied using `strcpy` to the buffer at `$sp+0x1b4`.This buffer is 8 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16282	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_net, at 0x9d01827c, the value for the `dhcp` key is copied using `strcpy` to the buffer at `$sp+0x270`.This buffer is 16 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16289	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_utc, at 0x9d0193ac, the value for the `offset` key is copied using `strcpy` to the buffer at `$sp+0x2d0`.This buffer is 100 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16275	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd sn_grp, at 0x9d01758c, the value for the `grp` key is copied using `strcpy` to the buffer at `$sp+0x1b4`.This buffer is 8 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16288	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_time, at 0x9d018f60, the value for the `dst` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16287	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_time, at 0x9d018f00, the value for the `dstend` key is copied using `strcpy` to the buffer at `$sp+0x270`.This buffer is 16 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16286	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_time, at 0x9d018ea0, the value for the `dststart` key is copied using `strcpy` to the buffer at `$sp+0x280`.This buffer is 16 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-16284	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_name, at 0x9d018958, the value for the `city` key is copied using `strcpy` to the buffer at `$sp+0x290`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16283	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_name, at 0x9d0188a8, the value for the `name` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16285	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_time, at 0x9d018e58, the value for the `offset` key is copied using `strcpy` to the buffer at `$sp+0x2d0`.This buffer is 100 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16281	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_net, at 0x9d018234, the value for the `sub` key is copied using `strcpy` to the buffer at `$sp+0x2b0`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16280	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_net, at 0x9d0181ec, the value for the `gate` key is copied using `strcpy` to the buffer at `$sp+0x290`.This buffer is 32 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16279	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_net, at 0x9d0181a4, the value for the `port` key is copied using `strcpy` to the buffer at `$sp+0x280`.This buffer is 16 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16278	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd s_net, at 0x9d01815c, the value for the `ip` key is copied using `strcpy` to the buffer at `$sp+0x2d0`.This buffer is 100 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16277	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd sn_grp, at 0x9d017658, the value for the `gcmd` key is copied using `strcpy` to the buffer at `$sp+0x270`.This buffer is 16 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2017-16276	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd sn_grp, at 0x9d0175f4, the value for the `gbt` key is copied using `strcpy` to the buffer at `$sp+0x280`.This buffer is 16 bytes large, sending anything longer will cause a buffer overflow.	9.9	More Details
CVE-2022-4447	The Fontsy WordPress plugin through 1.8.6 does not properly sanitize and escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to a SQL injection.	9.8	More Details
CVE-2023-0297	Code Injection in GitHub repository pyload/pyload prior to 0.5.0b3.dev31.	9.8	More Details
CVE-2022-1812	Integer Overflow or Wraparound in GitHub repository publify/publify prior to 9.2.10.	9.8	More Details
CVE-2023-0299	Improper Input Validation in GitHub repository publify/publify prior to 9.2.10.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0307	Weak Password Requirements in GitHub repository thorsten/phpmyfaq prior to 3.1.10.	9.8	More Details
CVE-2022-23521	Git is distributed revision control system. gitattributes are a mechanism to allow defining attributes for paths. These attributes can be defined by adding a `.gitattributes` file to the repository, which contains a set of file patterns and the attributes that should be set for paths matching this pattern. When parsing gitattributes, multiple integer overflows can occur when there is a huge number of path patterns, a huge number of attributes for a single pattern, or when the declared attribute names are huge. These overflows can be triggered via a crafted `.gitattributes` file that may be part of the commit history. Git silently splits lines longer than 2KB when parsing gitattributes from a file, but not when parsing them from the index. Consequentially, the failure mode depends on whether the file exists in the working tree, the index or both. This integer overflow can result in arbitrary heap reads and writes, which may result in remote code execution. The problem has been patched in the versions published on 2023-01-17, going back to v2.30.7. Users are advised to upgrade. There are no known workarounds for this issue.	9.8	More Details
CVE-2023-22495	Izanami is a shared configuration service well-suited for micro-service architecture implementation. Attackers can bypass the authentication in this application when deployed using the official Docker image. Because a hard coded secret is used to sign the authentication token (JWT), an attacker could compromise another instance of Izanami. This issue has been patched in version 1.11.0.	9.8	More Details
CVE-2023-0311	Improper Authentication in GitHub repository thorsten/phpmyfaq prior to 3.1.10.	9.8	More Details
CVE-2022-4060	The User Post Gallery WordPress plugin through 2.19 does not limit what callback functions can be called by users, making it possible to any visitors to run code on sites running it.	9.8	More Details
CVE-2023-22357	Active debug code exists in OMRON CP1L-EL20DR-D all versions, which may lead to a command that is not specified in FINS protocol being executed without authentication. A remote unauthenticated attacker may read/write in arbitrary area of the device memory, which may lead to overwriting the firmware, causing a denial-of-service (DoS) condition, and/or arbitrary code execution.	9.8	More Details
CVE-2023-22727	CakePHP is a development framework for PHP web apps. In affected versions the `Cake\Database\Query::limit()` and `Cake\Database\Query::offset()` methods are vulnerable to SQL injection if passed un-sanitized user request data. This issue has been fixed in 4.2.12, 4.3.11, 4.4.10. Users are advised to upgrade. Users unable to upgrade may mitigate this issue by using CakePHP's Pagination library. Manually validating or casting parameters to these methods will also mitigate the issue.	9.8	More Details
CVE-2022-46475	D-Link DIR 645A1 1.06B01_Beta01 was discovered to contain a stack overflow via the service= variable in the genacgi_main function.	9.8	More Details
CVE-2022-43977	An issue was discovered on GE Grid Solutions MS3000 devices before 3.7.6.25p0_3.2.2.17p0_4.7p0. The debug port accessible via TCP (a qconn service) lacks access control.	9.8	More Details
CVE-2022-43976	An issue was discovered in FC46-WebBridge on GE Grid Solutions MS3000 devices before 3.7.6.25p0_3.2.2.17p0_4.7p0. Direct access to the API is possible on TCP port 8888 via programs located in the cgi-bin folder without any authentication.	9.8	More Details
CVE-2022-47853	TOTOlink A7100RU V7.4cu.2313_B20191024 is vulnerable to Command Injection Vulnerability in the httpd service. An attacker can obtain a stable root shell through a specially constructed payload.	9.8	More Details
CVE-2022-23739	An incorrect authorization vulnerability was identified in GitHub Enterprise Server, allowing for escalation of privileges in GraphQL API requests from GitHub Apps. This vulnerability allowed an app installed on an organization to gain access to and modify most organization-level resources that are not tied to a repository regardless of granted permissions, such as users and organization-wide projects. Resources associated with repositories were not impacted, such as repository file content, repository-specific projects, issues, or pull requests. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.7.1 and was fixed in versions 3.3.16, 3.4.11, 3.5.8, 3.6.4, 3.7.1. This vulnerability was reported via the GitHub Bug Bounty program.	9.8	More Details
CVE-2023-22303	TP-Link SG105PE firmware prior to 'TL-SG105PE(UN) 1.0_1.0.0 Build 20221208' contains an authentication bypass vulnerability. Under the certain conditions, an attacker may impersonate an administrator of the product. As a result, information may be obtained and/or the product's settings may be altered with the privilege of the administrator.	9.8	More Details
CVE-2022-46955	Dynamic Transaction Queuing System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/ajax.php?action=save_queue.	9.8	More Details
CVE-2023-22279	MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allow a remote unauthenticated attacker to execute an arbitrary OS command.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45299	An issue in the IpFile argument of rust-lang webbrowser-rs v0.8.2 allows attackers to access arbitrary files via supplying a crafted URL.	9.8	More Details
CVE-2022-48252	The jokob-sk/Pi.Alert fork (before 22.12.20) of Pi.Alert allows Remote Code Execution via nmap_scan.php (scan parameter) OS Command Injection.	9.8	More Details
CVE-2022-46954	Dynamic Transaction Queuing System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/ajax.php?action=delete_transaction.	9.8	More Details
CVE-2022-4873	On Netcomm router models NF20MESH, NF20, and NL1902 a stack based buffer overflow affects the sessionKey parameter. By providing a specific number of bytes, the instruction pointer is able to be overwritten on the stack and crashes the application at a known location.	9.8	More Details
CVE-2022-47865	Lead Management System v1.0 is vulnerable to SQL Injection via the id parameter in removeOrder.php.	9.8	More Details
CVE-2022-47866	Lead management system v1.0 is vulnerable to SQL Injection via the id parameter in removeBrand.php.	9.8	More Details
CVE-2022-47859	Lead Management System v1.0 is vulnerable to SQL Injection via the user_id parameter in changePassword.php.	9.8	More Details
CVE-2022-47860	Lead Management System v1.0 is vulnerable to SQL Injection via the id parameter in removeProduct.php.	9.8	More Details
CVE-2022-47861	Lead Management System v1.0 is vulnerable to SQL Injection via the id parameter in removeLead.php.	9.8	More Details
CVE-2022-47862	Lead Management System v1.0 is vulnerable to SQL Injection via the customer_id parameter in ajax_represent.php.	9.8	More Details
CVE-2022-47864	Lead Management System v1.0 is vulnerable to SQL Injection via the id parameter in removeCategories.php.	9.8	More Details
CVE-2022-4498	In TP-Link routers, Archer C5 and WR710N-V1, running the latest available code, when receiving HTTP Basic Authentication the httpd service can be sent a crafted packet that causes a heap overflow. This can result in either a DoS (by crashing the httpd process) or an arbitrary code execution.	9.8	More Details
CVE-2022-48253	nhttpd in Nostromo before 2.1 is vulnerable to a path traversal that may allow an attacker to execute arbitrary commands on the remote server. The vulnerability occurs when the homedirs option is used.	9.8	More Details
CVE-2022-3515	A vulnerability was found in the Libksba library due to an integer overflow within the CRL parser. The vulnerability can be exploited remotely for code execution on the target system by passing specially crafted data to the application, for example, a malicious S/MIME attachment.	9.8	More Details
CVE-2022-39184	EXFO - BV-10 Performance Endpoint Unit authentication bypass User can manually manipulate access enabling authentication bypass.	9.8	More Details
CVE-2022-39185	EXFO - BV-10 Performance Endpoint Unit Undocumented privileged user. Unit has an undocumented hard-coded privileged user.	9.8	More Details
CVE-2022-41778	Delta Electronics InfraSuite Device Master versions 00.00.01a and prior deserialize user-supplied data provided through the Device-DataCollect service port without proper verification. An attacker could provide malicious serialized objects to execute arbitrary code upon deserialization.	9.8	More Details
CVE-2022-46471	Online Health Care System v1.0 was discovered to contain a SQL injection vulnerability via the consulting_id parameter at /healthcare/Admin/consulting_detail.php.	9.8	More Details
CVE-2022-46478	The RPC interface in datax-web v1.0.0 and v2.0.0 to v2.1.2 contains no permission checks by default which allows attackers to execute arbitrary commands via crafted Hessian serialized data.	9.8	More Details
CVE-2022-46502	Online Student Enrollment System v1.0 was discovered to contain a SQL injection vulnerability via the username parameter at /student_enrollment/admin/login.php.	9.8	More Details
CVE-2023-23566	A 2-Step Verification problem in Axigen 10.3.3.52 allows an attacker to access a mailbox by bypassing 2-Step Verification when they try to add an account to any third-party webmail service (or add an account to Outlook or Gmail, etc.) with IMAP or POP3 without any verification code.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41903	Git is distributed revision control system. `git log` can display commits in an arbitrary format using its `--format` specifiers. This functionality is also exposed to `git archive` via the `export-subst` gitattribute. When processing the padding operators, there is a integer overflow in `pretty.c::format_and_pad_commit()` where a `size_t` is stored improperly as an `int`, and then added as an offset to a `memcpy()`. This overflow can be triggered directly by a user running a command which invokes the commit formatting machinery (e.g., `git log --format=...`). It may also be triggered indirectly through git archive via the export-subst mechanism, which expands format specifiers inside of files within the repository during a git archive. This integer overflow can result in arbitrary heap writes, which may result in arbitrary code execution. The problem has been patched in the versions published on 2023-01-17, going back to v2.30.7. Users are advised to upgrade. Users who are unable to upgrade should disable `git archive` in untrusted repositories. If you expose git archive via `git daemon`, disable it by running `git config --global daemon.uploadArch false`.	9.8	More Details
CVE-2021-3966	usb device bluetooth class includes a buffer overflow related to implementation of net_buf_add_mem.	9.6	More Details
CVE-2022-43462	Auth. SQL Injection (SQLi) vulnerability in Adeel Ahmed's IP Blacklist Cloud plugin <= 5.00 versions.	9.1	More Details
CVE-2022-3782	keycloak: path traversal via double URL encoding. A flaw was found in Keycloak, where it does not properly validate URLs included in a redirect. An attacker can use this flaw to construct a malicious request to bypass validation and access other URLs and potentially sensitive information within the domain or possibly conduct further attacks. This flaw affects any client that utilizes a wildcard in the Valid Redirect URIs field.	9.1	More Details
CVE-2022-4101	The Images Optimize and Upload CF7 WordPress plugin through 2.1.4 does not validate the file to be deleted via an AJAX action available to unauthenticated users, which could allow them to delete arbitrary files on the server via path traversal attack.	9.1	More Details
CVE-2022-36760	Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-4428	support_uri parameter in the WARP client local settings file (mdm.xml) lacked proper validation which allowed for privilege escalation and launching an arbitrary executable on the local machine upon clicking on the "Send feedback" option. An attacker with access to the local file system could use a crafted XML config file pointing to a malicious file or set a local path to the executable using Cloudflare Zero Trust Dashboard (for Zero Trust enrolled clients).	8.9	More Details
CVE-2023-22850	Tiki before 24.1, when the Spreadsheets feature is enabled, allows lib/sheet/grid.php PHP Object Injection because of an unserialize call.	8.8	More Details
CVE-2022-43719	Two legacy REST API endpoints for approval and request access are vulnerable to cross site request forgery. This issue affects Apache Superset version 1.5.2 and prior versions and version 2.0.0.	8.8	More Details
CVE-2023-22853	Tiki before 24.1, when feature_create_webhelp is enabled, allows lib/structures/structlib.php PHP Object Injection because of an eval.	8.8	More Details
CVE-2017-16261	Multiple exploitable buffer overflow vulnerabilities exist in the PubNub message handler for the "cc" channel of Insteon Hub running firmware version 1012. Specially crafted commands sent through the PubNub service can cause a stack-based buffer overflow overwriting arbitrary data. An attacker should send an authenticated HTTP request to trigger this vulnerability. In cmd g_b, at 0x9d015714, the value for the `grp` key is copied using `strcpy` to the buffer at `$sp+0x280`.This buffer is 16 bytes large, sending anything longer will cause a buffer overflow.	8.8	More Details
CVE-2022-41955	Autolab is a course management service, initially developed by a team of students at Carnegie Mellon University, that enables instructors to offer autograded programming assignments to their students over the Web. A remote code execution vulnerability was discovered in Autolab's MOSS functionality, whereby an instructor with access to the feature might be able to execute code on the server hosting Autolab. This vulnerability has been patched in version 2.10.0. As a workaround, disable the MOSS feature if it is unneeded by replacing the body of `run_moss` in `app/controllers/courses_controller.rb` with `render(plain: "Feature disabled", status: :bad_request) && return`.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22493	RSSHub is an open source RSS feed generator. RSSHub is vulnerable to Server-Side Request Forgery (SSRF) attacks. This vulnerability allows an attacker to send arbitrary HTTP requests from the server to other servers or resources on the network. An attacker can exploit this vulnerability by sending a request to the affected routes with a malicious URL. An attacker could also use this vulnerability to send requests to internal or any other servers or resources on the network, potentially gain access to sensitive information that would not normally be accessible and amplifying the impact of the attack. The patch for this issue can be found in commit a66cbcf.	8.8	More Details
CVE-2023-22952	In SugarCRM before 12.0. Hotfix 91155, a crafted request can inject custom PHP code through the EmailTemplates because of missing input validation.	8.8	More Details
CVE-2022-46891	An issue was discovered in the Arm Mali GPU Kernel Driver. There is a use-after-free. A non-privileged user can make improper GPU processing operations to gain access to already freed memory. This affects Midgard r13p0 through r32p0, Bifrost r1p0 through r40p0, and Valhall r19p0 through r40p0.	8.8	More Details
CVE-2023-22959	WebChess through 0.9.0 and 1.0.0.rc2 allows SQL injection: mainmenu.php, chess.php, and opponentspassword.php (txtFirstName, txtLastName).	8.8	More Details
CVE-2023-0294	The Mediamatic – Media Library Folders plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.8.1. This is due to missing or incorrect nonce validation on its AJAX actions function. This makes it possible for unauthenticated attackers to change image categories used by the plugin, via forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2022-40983	An integer overflow vulnerability exists in the QML QtScript Reflect API of Qt Project Qt 6.3.2. A specially-crafted javascript code can trigger an integer overflow during memory allocation, which can lead to arbitrary code execution. Target application would need to access a malicious web page to trigger this vulnerability.	8.8	More Details
CVE-2023-0315	Command Injection in GitHub repository froxlor/froxlor prior to 2.0.8.	8.8	More Details
CVE-2022-43591	A buffer overflow vulnerability exists in the QML QtScript Reflect API of Qt Project Qt 6.3.2. A specially-crafted javascript code can trigger an out-of-bounds memory access, which can lead to arbitrary code execution. Target application would need to access a malicious web page to trigger this vulnerability.	8.8	More Details
CVE-2022-42136	Authenticated mail users, under specific circumstances, could add files with unsanitized content in public folders where the IIS user had permission to access. That action, could lead an attacker to store arbitrary code on that files and execute RCE commands.	8.8	More Details
CVE-2022-43389	A buffer overflow vulnerability in the library of the web server in Zyxel NR7101 firmware prior to V1.15(ACCC.3)C0, which could allow an unauthenticated attacker to execute some OS commands or to cause denial-of-service (DoS) conditions on a vulnerable device.	8.6	More Details
CVE-2022-41953	Git GUI is a convenient graphical tool that comes with Git for Windows. Its target audience is users who are uncomfortable with using Git on the command-line. Git GUI has a function to clone repositories. Immediately after the local clone is available, Git GUI will automatically post-process it, among other things running a spell checker called `aspell.exe` if it was found. Git GUI is implemented as a Tcl/Tk script. Due to the unfortunate design of Tcl on Windows, the search path when looking for an executable _always includes the current directory_. Therefore, malicious repositories can ship with an `aspell.exe` in their top-level directory which is executed by Git GUI without giving the user a chance to inspect it first, i.e. running untrusted code. This issue has been addressed in version 2.39.1. Users are advised to upgrade. Users unable to upgrade should avoid using Git GUI for cloning. If that is not a viable option, at least avoid cloning from untrusted sources.	8.6	More Details
CVE-2017-14454	Multiple exploitable buffer overflow vulnerabilities exists in the PubNub message handler for the "control" channel of Insteon Hub running firmware version 1012. Specially crafted replies received from the PubNub service can cause buffer overflows on a global section overwriting arbitrary data. An attacker should impersonate PubNub and answer an HTTPS GET request to trigger this vulnerability. The `strcpy` at [18] overflows the buffer `insteon_pubnub.channel_al`, which has a size of 16 bytes.	8.5	More Details
CVE-2023-22875	IBM QRadar SIEM 7.4 and 7.5copies certificate key files used for SSL/TLS in the QRadar web user interface to managed hosts in the deployment that do not require that key. IBM X-Force ID: 244356.	8.4	More Details
CVE-2022-34440	Dell EMC SCG Policy Manager, versions from 5.10 to 5.12, contain(s) a contain a Hard-coded Cryptographic Key vulnerability. An attacker with the knowledge of the hard-coded sensitive information, could potentially exploit this vulnerability to login to the system to gain admin privileges.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42271	NVIDIA BMC contains a vulnerability in IPMI handler, where an authorized attacker can cause a buffer overflow and cause a denial of service or gain code execution	8.4	More Details
CVE-2022-2893	RONDS EPM version 1.19.5 does not properly validate the filename parameter, which could allow an unauthorized user to specify file paths and download files.	8.2	More Details
CVE-2022-43393	An improper check for unusual or exceptional conditions in the HTTP request processing function of Zyxel GS1920-24v2 firmware prior to V4.70(ABMH.8)C0, which could allow an unauthenticated attacker to corrupt the contents of the memory and result in a denial-of-service (DoS) condition on a vulnerable device.	8.2	More Details
CVE-2022-46093	Hospital Management System v1.0 is vulnerable to SQL Injection. Attackers can gain administrator privileges without the need for a password.	8.2	More Details
CVE-2023-22491	Gatsby is a free and open source framework based on React that helps developers build websites and apps. The gatsby-transformer-remark plugin prior to versions 5.25.1 and 6.3.2 passes input through to the `gray-matter` npm package, which is vulnerable to JavaScript injection in its default configuration, unless input is sanitized. The vulnerability is present in gatsby-transformer-remark when passing input in data mode (querying MarkdownRemark nodes via GraphQL). Injected JavaScript executes in the context of the build server. To exploit this vulnerability untrusted/unsanitized input would need to be sourced by or added into a file processed by gatsby-transformer-remark. A patch has been introduced in `gatsby-transformer-remark@5.25.1` and `gatsby-transformer-remark@6.3.2` which mitigates the issue by disabling the `gray-matter` JavaScript Frontmatter engine. As a workaround, if an older version of `gatsby-transformer-remark` must be used, input passed into the plugin should be sanitized ahead of processing. It is encouraged for projects to upgrade to the latest major release branch for all Gatsby plugins to ensure the latest security updates and bug fixes are received in a timely manner.	8.1	More Details
CVE-2022-42272	NVIDIA BMC contains a vulnerability in IPMI handler, where an authorized attacker can cause a buffer overflow, which may lead to code execution, denial of service or escalation of privileges.	8.1	More Details
CVE-2022-42273	NVIDIA BMC contains a vulnerability in libwebsocket, where an authorized attacker can cause a buffer overflow and cause a denial of service or gain code execution.	8.1	More Details
CVE-2023-22496	Netdata is an open source option for real-time infrastructure monitoring and troubleshooting. An attacker with the ability to establish a streaming connection can execute arbitrary commands on the targeted Netdata agent. When an alert is triggered, the function `health_alarm_execute` is called. This function performs different checks and then enqueues a command by calling `spawn_enq_cmd`. This command is populated with several arguments that are not sanitized. One of them is the `registry_hostname` of the node for which the alert is raised. By providing a specially crafted `registry_hostname` as part of the health data that is streamed to a Netdata (parent) agent, an attacker can execute arbitrary commands at the remote host as a side-effect of the raised alert. Note that the commands are executed as the user running the Netdata Agent. This user is usually named `netdata`. The ability to run arbitrary commands may allow an attacker to escalate privileges by escalating other vulnerabilities in the system, as that user. The problem has been fixed in: Netdata agent v1.37 (stable) and Netdata agent v1.36.0-409 (nightly). As a workaround, streaming is not enabled by default. If you have previously enabled this, it can be disabled. Limiting access to the port on the recipient Agent to trusted child connections may mitigate the impact of this vulnerability.	8.1	More Details
CVE-2023-22286	Cross-site request forgery (CSRF) vulnerability in MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to hijack the user authentication and conduct user's unintended operations by having a user to view a malicious page while logged in.	8.1	More Details
CVE-2022-46648	ruby-git versions prior to v1.13.0 allows a remote authenticated attacker to execute an arbitrary ruby code by having a user to load a repository containing a specially crafted filename to the product. This vulnerability is different from CVE-2022-47318.	8.0	More Details
CVE-2022-34441	Dell EMC SCG Policy Manager, versions from 5.10 to 5.12, contain(s) a contain a Hard-coded Cryptographic Key vulnerability. An attacker with the knowledge of the hard-coded sensitive information, could potentially exploit this vulnerability to login to the system to gain admin privileges.	8.0	More Details
CVE-2022-47318	ruby-git versions prior to v1.13.0 allows a remote authenticated attacker to execute an arbitrary ruby code by having a user to load a repository containing a specially crafted filename to the product. This vulnerability is different from CVE-2022-46648.	8.0	More Details
CVE-2023-22304	OS command injection vulnerability in PIX-RT100 versions RT100_TEQ_2.1.1_EQ101 and RT100_TEQ_2.1.2_EQ101 allows a network-adjacent attacker who can access product settings to execute an arbitrary OS command.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21594	Adobe InCopy versions 18.0 (and earlier), 17.4 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-21597	Adobe InCopy versions 18.0 (and earlier), 17.4 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-21596	Adobe InCopy versions 18.0 (and earlier), 17.4 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-3087	Fuji Electric Tellus Lite V-Simulator versions 4.0.12.0 and prior are vulnerable to an out-of-bounds write which may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2023-21595	Adobe InCopy versions 18.0 (and earlier), 17.4 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-22366	CX-Motion-MCH v2.32 and earlier contains an access of uninitialized pointer vulnerability. Having a user to open a specially crafted project file may lead to information disclosure and/or arbitrary code execution.	7.8	More Details
CVE-2023-21587	Adobe InDesign version 18.0 (and earlier), 17.4 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-3977	A use-after-free flaw was found in the Linux kernel MCTP (Management Component Transport Protocol) functionality. This issue occurs when a user simultaneously calls DROPTAG ioctl and socket close happens, which could allow a local user to crash the system or potentially escalate their privileges on the system.	7.8	More Details
CVE-2023-0247	Uncontrolled Search Path Element in GitHub repository bits-and-blooms/bloom prior to 3.3.1.	7.8	More Details
CVE-2021-36204	Under some circumstances an Insufficiently Protected Credentials vulnerability in Johnson Controls Metasys ADS/ADX/OAS 10 versions prior to 10.1.6 and 11 versions prior to 11.0.3 allows API calls to expose credentials in plain text.	7.8	More Details
CVE-2022-4258	In multiple versions of HIMA PC based Software an unquoted Windows search path vulnerability might allow local users to gain privileges via a malicious .exe file and gain full access to the system.	7.8	More Details
CVE-2022-3159	The APDFL.dll contains a stack-based buffer overflow vulnerability that could be triggered while parsing specially crafted PDF files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2022-3160	The APDFL.dll contains an out-of-bounds write past the fixed-length heap-based buffer while parsing specially crafted PDF files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-0302	Failure to Sanitize Special Elements into a Different Plane (Special Element Injection) in GitHub repository radareorg/radare2 prior to 5.8.2.	7.8	More Details
CVE-2022-3161	The APDFL.dll contains a memory corruption vulnerability while parsing specially crafted PDF files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2022-42274	NVIDIA BMC contains a vulnerability in IPMI handler, where an authorized attacker can cause a buffer overflow and cause a denial of service or gain code execution.	7.8	More Details
CVE-2023-21590	Adobe InDesign version 18.0 (and earlier), 17.4 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21589	Adobe InDesign version 18.0 (and earlier), 17.4 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-3841	RHACM: unauthenticated SSRF in console API endpoint. A Server-Side Request Forgery (SSRF) vulnerability was found in the console API endpoint from Red Hat Advanced Cluster Management for Kubernetes (RHACM). An attacker could take advantage of this as the console API endpoint is missing an authentication check, allowing unauthenticated users making requests.	7.8	More Details
CVE-2022-42268	Omniverse Kit contains a vulnerability in the reference applications Create, Audio2Face, Isaac Sim, View, Code, and Machinima. These applications allow executable Python code to be embedded in Universal Scene Description (USD) files to customize all aspects of a scene. If a user opens a USD file that contains embedded Python code in one of these applications, the embedded Python code automatically runs with the privileges of the user who opened the file. As a result, an unprivileged remote attacker could craft a USD file containing malicious Python code and persuade a local user to open the file, which may lead to information disclosure, data tampering, and denial of service.	7.8	More Details
CVE-2023-21588	Adobe InDesign version 18.0 (and earlier), 17.4 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-0288	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.1189.	7.8	More Details
CVE-2023-23559	In rndis_query_oid in drivers/net/wireless/rndis_wlan.c in the Linux kernel through 6.1.5, there is an integer overflow in an addition.	7.8	More Details
CVE-2022-46623	Judging Management System v1.0.0 was discovered to contain a SQL injection vulnerability via the username parameter.	7.8	More Details
CVE-2022-3650	A privilege escalation flaw was found in Ceph. Ceph-crash.service allows a local attacker to escalate privileges to root in the form of a crash dump, and dump privileged information.	7.8	More Details
CVE-2022-4696	There exists a use-after-free vulnerability in the Linux kernel through io_uring and the IORING_OP_SPLICE operation. If IORING_OP_SPLICE is missing the IO_WQ_WORK_FILES flag, which signals that the operation won't use current->nsproxy, so its reference counter is not increased. This assumption is not always true as calling io_splice on specific files will call the get_uts function which will use current->nsproxy leading to invalidly decreasing its reference counter later causing the use-after-free vulnerability. We recommend upgrading to version 5.10.160 or above	7.8	More Details
CVE-2021-26316	Failure to validate the communication buffer and communication service in the BIOS may allow an attacker to tamper with the buffer resulting in potential SMM (System Management Mode) arbitrary code execution.	7.8	More Details
CVE-2021-26398	Insufficient input validation in SYS_KEY_DERIVE system call in a compromised user application or ABL may allow an attacker to corrupt ASP (AMD Secure Processor) OS memory which may lead to potential arbitrary code execution.	7.8	More Details
CVE-2021-26409	Insufficient bounds checking in SEV-ES may allow an attacker to corrupt Reverse Map table (RMP) memory, potentially resulting in a loss of SNP (Secure Nested Paging) memory integrity.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22487	Flarum is a forum software for building communities. Using the mentions feature provided by the flarum/mentions extension, users can mention any post ID on the forum with the special `@"<username>"#p<id>` syntax. The following behavior never changes no matter if the actor should be able to read the mentioned post or not: A URL to the mentioned post is inserted into the actor post HTML, leaking its discussion ID and post number. The `mentionsPosts` relationship included in the `POST /api/posts` and `PATCH /api/posts/<id>` JSON responses leaks the full JSON:API payload of all mentioned posts without any access control. This includes the content, date, number and attributes added by other extensions. An attacker only needs the ability to create new posts on the forum to exploit the vulnerability. This works even if new posts require approval. If they have the ability to edit posts, the attack can be performed even more discreetly by using a single post to scan any size of database and hiding the attack post content afterward. The attack allows the leaking of all posts in the forum database, including posts awaiting approval, posts in tags the user has no access to, and private discussions created by other extensions like FriendsOfFlarum Byobu. This also includes non-comment posts like tag changes or renaming events. The discussion payload is not leaked but using the mention HTML payload it's possible to extract the discussion ID of all posts and combine all posts back together into their original discussions even if the discussion title remains unknown. All Flarum versions prior to 1.6.3 are affected. The vulnerability has been fixed and published as flarum/core v1.6.3. As a workaround, user can disable the mentions extension.	7.7	More Details
CVE-2017-5242	Nexpose and InsightVM virtual appliances downloaded between April 5th, 2017 and May 3rd, 2017 contain identical SSH host keys. Normally, a unique SSH host key should be generated the first time a virtual appliance boots.	7.7	More Details
CVE-2022-42275	NVIDIA BMC IPMI handler allows an unauthenticated host to write to a host SPI flash bypassing secureboot protections. This may lead to a loss of integrity and denial of service.	7.7	More Details
CVE-2023-23637	IMPatienT before 1.5.2 allows stored XSS via onmouseover in certain text fields within a PATCH /modify_onto request to the ontology builder. This may allow attackers to steal Protected Health Information.	7.6	More Details
CVE-2023-22417	A Missing Release of Memory after Effective Lifetime vulnerability in the Flow Processing Daemon (flowd) of Juniper Networks Junos OS allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS). In an IPsec VPN environment, a memory leak will be seen if a DH or ECDH group is configured. Eventually the flowd process will crash and restart. This issue affects Juniper Networks Junos OS on SRX Series: All versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S8, 19.4R3-S10; 20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2.	7.5	More Details
CVE-2023-22412	An Improper Locking vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series with MS-MPC or MS-MIC card and SRX Series allows an unauthenticated, network-based attacker to cause a flow processing daemon (flowd) crash and thereby a Denial of Service (DoS). Continued receipt of these specific packets will cause a sustained Denial of Service condition. This issue occurs when SIP ALG is enabled and specific SIP messages are processed simultaneously. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1 on MX Series, or SRX Series.	7.5	More Details
CVE-2023-22413	An Improper Check or Handling of Exceptional Conditions vulnerability in the IPsec library of Juniper Networks Junos OS allows a network-based, unauthenticated attacker to cause Denial of Service (DoS). On all MX platforms with MS-MPC or MS-MIC card, when specific IPv4 packets are processed by an IPsec6 tunnel, the Multiservices PIC Management Daemon (mspmand) process will core and restart. This will lead to FPC crash. Traffic flow is impacted while mspmand restarts. Continued receipt of these specific packets will cause a sustained Denial of Service (DoS) condition. This issue only occurs if an IPv4 address is not configured on the multiservice interface. This issue affects: Juniper Networks Junos OS on MX Series All versions prior to 19.4R3-S9; 20.1 version 20.1R3-S5 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R2.	7.5	More Details
CVE-2023-22415	An Out-of-Bounds Write vulnerability in the H.323 ALG of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause Denial of Service (DoS). On all MX Series and SRX Series platform, when H.323 ALG is enabled and specific H.323 packets are received simultaneously, a flow processing daemon (flowd) crash will occur. Continued receipt of these specific packets will cause a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series All versions prior to 19.4R3-S10; 20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2-S1, 22.1R3; 22.2 versions prior to 22.2R1-S2, 22.2R2.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22416	A Buffer Overflow vulnerability in SIP ALG of Juniper Networks Junos OS allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS). On all MX Series and SRX Series platform with SIP ALG enabled, when a malformed SIP packet is received, the flow processing daemon (flowd) will crash and restart. This issue affects: Juniper Networks Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R3-S1; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R1-S2, 22.1R2; 22.2 versions prior to 22.2R1-S1, 22.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1 on SRX Series.	7.5	More Details
CVE-2023-23749	The 'LDAP Integration with Active Directory and OpenLDAP - NTLM & Kerberos Login' extension is vulnerable to LDAP Injection since is not properly sanitizing the 'username' POST parameter. An attacker can manipulate this paramter to dump arbitrary contents form the LDAP Database.	7.5	More Details
CVE-2022-42276	NVIDIA DGX A100 contains a vulnerability in SBIOS in the SmiFlash, where a local user with elevated privileges can read, write and erase flash, which may lead to code execution, escalation of privileges, denial of service, and information disclosure. The scope of impact can extend to other components.	7.5	More Details
CVE-2022-48256	Technitium DNS Server before 10.0 allows a self-CNAME denial-of-service attack in which a CNAME loop causes an answer to contain hundreds of records.	7.5	More Details
CVE-2023-22411	An Out-of-Bounds Write vulnerability in Flow Processing Daemon (flowd) of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to cause Denial of Service (DoS). On SRX Series devices using Unified Policies with IPv6, when a specific IPv6 packet goes through a dynamic-application filter which will generate an ICMP deny message, the flowd core is observed and the PFE is restarted. This issue affects: Juniper Networks Junos OS on SRX Series: 19.2 versions prior to 19.2R3-S6; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S4; 20.4 versions prior to 20.4R3-S3; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2; 21.4 versions prior to 21.4R2.	7.5	More Details
CVE-2006-20001	A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash. This issue affects Apache HTTP Server 2.4.54 and earlier.	7.5	More Details
CVE-2023-22624	Zoho ManageEngine Exchange Reporter Plus before 5708 allows attackers to conduct XXE attacks.	7.5	More Details
CVE-2022-3091	RONDS EPM version 1.19.5 has a vulnerability in which a function could allow unauthenticated users to leak credentials. In some circumstances, an attacker can exploit this vulnerability to execute operating system (OS) commands.	7.5	More Details
CVE-2023-20530	Insufficient input validation of BIOS mailbox messages in SMU may result in out-of-bounds memory reads potentially resulting in a denial of service.	7.5	More Details
CVE-2023-22410	A Missing Release of Memory after Effective Lifetime vulnerability in the Juniper Networks Junos OS on MX Series platforms with MPC10/MPC11 line cards, allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS). Devices are only vulnerable when the Suspicious Control Flow Detection (scfd) feature is enabled. Upon enabling this specific feature, an attacker sending specific traffic is causing memory to be allocated dynamically and it is not freed. Memory is not freed even after deactivating this feature. Sustained processing of such traffic will eventually lead to an out of memory condition that prevents all services from continuing to function, and requires a manual restart to recover. The FPC memory usage can be monitored using the CLI command "show chassis fpc". On running the above command, the memory of AftDdosScfdFlow can be observed to detect the memory leak. This issue affects Juniper Networks Junos OS on MX Series: All versions prior to 20.2R3-S5; 20.3 version 20.3R1 and later versions.	7.5	More Details
CVE-2023-22399	When sFlow is enabled and it monitors a packet forwarded via ECMP, a buffer management vulnerability in the dcpfe process of Juniper Networks Junos OS on QFX10K Series systems allows an attacker to cause the Packet Forwarding Engine (PFE) to crash and restart by sending specific genuine packets to the device, resulting in a Denial of Service (DoS) condition. The dcpfe process tries to copy more data into a smaller buffer, which overflows and corrupts the buffer, causing a crash of the dcpfe process. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS on QFX10K Series: All versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2-S2, 21.4R3; 22.1 versions prior to 22.1R2; 22.2 versions prior to 22.2R1-S2, 22.2R2.	7.5	More Details
CVE-2022-46463	An access control issue in Harbor v1.X.X to v2.5.3 allows attackers to access public and private image repositories without authentication. NOTE: the vendor's position is that this "is clearly described in the documentation as a feature."	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22391	A vulnerability in class-of-service (CoS) queue management in Juniper Networks Junos OS on the ACX2K Series devices allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). Specific packets are being incorrectly routed to a queue used for other high-priority traffic such as BGP, PIM, ICMP, ICMPV6 ND and ISAKMP. Due to this misclassification of traffic, receipt of a high rate of these specific packets will cause delays in the processing of other traffic, leading to a Denial of Service (DoS). Continued receipt of this amount of traffic will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS on ACX2K Series: All versions prior to 19.4R3-S9; All 20.2 versions; 20.3 versions prior to 20.3R3-S6 on ACX2K Series; 20.4 versions prior to 20.4R3-S4 on ACX2K Series; All 21.1 versions; 21.2 versions prior to 21.2R3-S3 on ACX2K Series. Note: This issues affects legacy ACX2K Series PPC-based devices. This platform reached Last Supported Version (LSV) as of the Junos OS 21.2 Release.	7.5	More Details
CVE-2023-22393	An Improper Check for Unusual or Exceptional Conditions vulnerability in BGP route processing of Juniper Networks Junos OS and Junos OS Evolved allows an attacker to cause Routing Protocol Daemon (RPD) crash by sending a BGP route with invalid next-hop resulting in a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects systems without import policy configured. This issue affects: Juniper Networks Junos OS 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R2-S2, 21.4R3; 22.1 versions prior to 22.1R1-S2, 22.1R2; 22.2 versions prior to 22.2R1-S1, 22.2R2. Juniper Networks Junos OS Evolved 21.4-EVO versions prior to 21.4R2-S2-EVO, 21.4R3-EVO; 22.1-EVO versions prior to 22.1R1-S2-EVO, 22.1R2-EVO; 22.2-EVO versions prior to 22.2R1-S1-EVO, 22.2R2-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 21.1R1. Juniper Networks Junos OS Evolved versions prior to 21.3R1-EVO.	7.5	More Details
CVE-2023-22394	An Improper Handling of Unexpected Data Type vulnerability in the handling of SIP calls in Juniper Networks Junos OS on SRX Series and MX Series platforms allows an attacker to cause a memory leak leading to Denial of Services (DoS). This issue occurs on all MX Series platforms with MS-MPC or MS-MIC card and all SRX Series platforms where SIP ALG is enabled. Successful exploitation of this vulnerability prevents additional SIP calls and applications from succeeding. The SIP ALG needs to be enabled, either implicitly / by default or by way of configuration. To confirm whether SIP ALG is enabled on SRX use the following command: user@host> show security alg status | match sip SIP : Enabled This issue affects Juniper Networks Junos OS on SRX Series and on MX Series: All versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S8, 19.4R3-S10; 20.1 versions 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S5; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R2-S2, 21.4R3; 22.1 versions prior to 22.1R1-S2, 22.1R2, 22.1R3-S1. This issue does not affect Juniper Networks Junos OS on SRX Series and on MX Series: All versions prior to 18.2R1.	7.5	More Details
CVE-2023-22396	An Uncontrolled Resource Consumption vulnerability in TCP processing on the Routing Engine (RE) of Juniper Networks Junos OS allows an unauthenticated network-based attacker to send crafted TCP packets destined to the device, resulting in an MBUF leak that ultimately leads to a Denial of Service (DoS). The system does not recover automatically and must be manually restarted to restore service. This issue occurs when crafted TCP packets are sent directly to a configured IPv4 or IPv6 interface on the device. Transit traffic will not trigger this issue. MBUF usage can be monitored through the use of the 'show system buffers' command. For example: user@junos> show system buffers | refresh 5 4054/566/4620 mbufs in use (current/cache/total) ... 4089/531/4620 mbufs in use (current/cache/total) ... 4151/589/4740 mbufs in use (current/cache/total) ... 4213/527/4740 mbufs in use (current/cache/total) This issue affects Juniper Networks Junos OS: 12.3 version 12.3R12-S19 and later versions; 15.1 version 15.1R7-S10 and later versions; 17.3 version 17.3R3-S12 and later versions; 18.4 version 18.4R3-S9 and later versions; 19.1 version 19.1R3-S7 and later versions; 19.2 version 19.2R3-S3 and later versions; 19.3 version 19.3R2-S7, 19.3R3-S3 and later versions prior to 19.3R3-S7; 19.4 version 19.4R2-S7, 19.4R3-S5 and later versions prior to 19.4R3-S10; 20.1 version 20.1R3-S1 and later versions; 20.2 version 20.2R3-S2 and later versions prior to 20.2R3-S6; 20.3 version 20.3R3-S1 and later versions prior to 20.3R3-S6; 20.4 version 20.4R2-S2, 20.4R3 and later versions prior to 20.4R3-S5; 21.1 version 21.1R2 and later versions prior to 21.1R3-S4; 21.2 version 21.2R1-S1, 21.2R2 and later versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2-S1, 22.1R3; 22.2 versions prior to 22.2R1-S2, 22.2R2; 22.3 versions prior to 22.3R1-S1, 22.3R2.	7.5	More Details
CVE-2023-20522	Insufficient input validation in ASP may allow an attacker with a malicious BIOS to potentially cause a denial of service.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22400	An Uncontrolled Resource Consumption vulnerability in the PFE management daemon (evo-pfemand) of Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to cause an FPC crash leading to a Denial of Service (DoS). When a specific SNMP GET operation or a specific CLI command is executed this will cause a GUID resource leak, eventually leading to exhaustion and result in an FPC crash and reboot. GUID exhaustion will trigger a syslog message like one of the following for example: evo-pfemand[<pid>]: get_next_guid: Ran out of Guid Space ... evo-aftmand-zx[<pid>]: get_next_guid: Ran out of Guid Space ... This leak can be monitored by running the following command and taking note of the value in the rightmost column labeled Guids: user@host> show platform application-info allocations app evo-pfemand | match "IFDIdIIFLIdlContext" Node Application Context Name Live Allocs Fails Guids re0 evo-pfemand net::juniper::interfaces::IFDId 0 3448 0 3448 re0 evo-pfemand net::juniper::interfaces::IFLId 0 561 0 561 user@host> show platform application-info allocations app evo-pfemand | match "IFDIdIIFLIdlContext" Node Application Context Name Live Allocs Fails Guids re0 evo-pfemand net::juniper::interfaces::IFDId 0 3784 0 3784 re0 evo-pfemand net::juniper::interfaces::IFLId 0 647 0 647 This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S3-EVO; 21.1-EVO version 21.1R1-EVO and later versions; 21.2-EVO versions prior to 21.2R3-S4-EVO; 21.3-EVO version 21.3R1-EVO and later versions; 21.4-EVO versions prior to 21.4R2-EVO.	7.5	More Details
CVE-2023-20531	Insufficient bound checks in the SMU may allow an attacker to update the SRAM from/to address space to an invalid value potentially resulting in a denial of service.	7.5	More Details
CVE-2022-4743	A potential memory leak issue was discovered in SDL2 in GLES_CreateTexture() function in SDL_render_gles.c. The vulnerability allows an attacker to cause a denial of service attack. The vulnerability affects SDL2 v2.0.4 and above. SDL-1.x are not affected.	7.5	More Details
CVE-2023-22401	An Improper Validation of Array Index vulnerability in the Advanced Forwarding Toolkit Manager daemon (aftmand) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). On the PTX10008 and PTX10016 platforms running Junos OS or Junos OS Evolved, when a specific SNMP MIB is queried this will cause a PFE crash and the FPC will go offline and not automatically recover. A system restart is required to get the affected FPC in an operational state again. This issue affects: Juniper Networks Junos OS 22.1 version 22.1R2 and later versions; 22.1 versions prior to 22.1R3; 22.2 versions prior to 22.2R2. Juniper Networks Junos OS Evolved 21.3-EVO version 21.3R3-EVO and later versions; 21.4-EVO version 21.4R1-S2-EVO, 21.4R2-EVO and later versions prior to 21.4R2-S1-EVO; 22.1-EVO version 22.1R2-EVO and later versions prior to 22.1R3-EVO; 22.2-EVO versions prior to 22.2R1-S1-EVO, 22.2R2-EVO.	7.5	More Details
CVE-2023-22403	An Allocation of Resources Without Limits or Throttling vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS). On QFX10K Series, Inter-Chassis Control Protocol (ICCP) is used in MC-LAG topologies to exchange control information between the devices in the topology. ICCP connection flaps and sync issues will be observed due to excessive specific traffic to the local device. This issue affects Juniper Networks Junos OS on QFX10K Series: * All versions prior to 20.2R3-S7; * 20.4 versions prior to 20.4R3-S4; * 21.1 versions prior to 21.1R3-S3; * 21.2 versions prior to 21.2R3-S1; * 21.3 versions prior to 21.3R3; * 21.4 versions prior to 21.4R3; * 22.1 versions prior to 22.1R2.	7.5	More Details
CVE-2023-22408	An Improper Validation of Array Index vulnerability in the SIP ALG of Juniper Networks Junos OS on SRX 5000 Series allows a network-based, unauthenticated attacker to cause a Denial of Service (DoS). When an attacker sends an SIP packets with a malformed SDP field then the SIP ALG can not process it which will lead to an FPC crash and restart. Continued receipt of these specific packets will lead to a sustained Denial of Service. This issue can only occur when both below mentioned conditions are fulfilled: 1. Call distribution needs to be enabled: [security alg sip enable-call-distribution] 2. The SIP ALG needs to be enabled, either implicitly / by default or by way of configuration. To confirm whether SIP ALG is enabled on SRX, and MX with SPC3 use the following command: user@host> show security alg status | match sip SIP : Enabled This issue affects Juniper Networks Junos OS on SRX 5000 Series: 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S2; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R3; 22.3 versions prior to 22.3R1-S1, 22.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.4R1.	7.5	More Details
CVE-2023-20529	Insufficient bound checks in the SMU may allow an attacker to update the from/to address space to an invalid value potentially resulting in a denial of service.	7.5	More Details
CVE-2022-25026	A Server-Side Request Forgery (SSRF) in Rocket TRUfusion Portal v7.9.2.1 allows remote attackers to gain access to sensitive resources on the internal network via a crafted HTTP request to /trufusionPortal/upDwModuleProxy.	7.5	More Details
CVE-2022-42277	NVIDIA DGX Station contains a vulnerability in SBIOS in the SmiFlash, where a local user with elevated privileges can read, write and erase flash, which may lead to code execution, escalation of privileges, denial of service, and information disclosure. The scope of impact can extend to other components.	7.5	More Details
CVE-2022-25027	The Forgotten Password functionality of Rocket TRUfusion Portal v7.9.2.1 allows remote attackers to bypass authentication and access restricted pages by validating the user's session token when the "Password forgotten?" button is clicked.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41860	In freeradius, when an EAP-SIM supplicant sends an unknown SIM option, the server will try to look that option up in the internal dictionaries. This lookup will fail, but the SIM code will not check for that failure. Instead, it will dereference a NULL pointer, and cause the server to crash.	7.5	More Details
CVE-2023-23590	Mercedes-Benz XENTRY Retail Data Storage 7.8.1 allows remote attackers to cause a denial of service (device restart) via an unauthenticated API request. The attacker must be on the same network as the device.	7.5	More Details
CVE-2023-23595	BlueCat Device Registration Portal 2.2 allows XXE attacks that exfiltrate single-line files. A single-line file might contain credentials, such as "machine example.com login daniel password qwerty" in the documentation example for the .netrc file format. NOTE: 2.x versions are no longer supported. There is no available information about whether any later version is affected.	7.5	More Details
CVE-2022-4874	Authentication bypass in Netcomm router models NF20MESH, NF20, and NL1902 allows an unauthenticated user to access content. In order to serve static content, the application performs a check for the existence of specific characters in the URL (.css, .png etc). If it exists, it performs a "fake login" to give the request an active session to load the file and not redirect to the login page.	7.5	More Details
CVE-2022-43975	An issue was discovered in FC46-WebBridge on GE Grid Solutions MS3000 devices before 3.7.6.25p0_3.2.2.17p0_4.7p0. A vulnerability in the web server allows arbitrary files and configurations to be read via directory traversal over TCP port 8888.	7.5	More Details
CVE-2022-41859	In freeradius, the EAP-PWD function compute_password_element() leaks information about the password which allows an attacker to substantially reduce the size of an offline dictionary attack.	7.5	More Details
CVE-2022-42967	Caret is vulnerable to an XSS attack when the user opens a crafted Markdown file when preview mode is enabled. This directly leads to client-side code execution.	7.5	More Details
CVE-2023-0122	A NULL pointer dereference vulnerability in the Linux kernel NVMe functionality, in nvmet_setup_auth(), allows an attacker to perform a Pre-Auth Denial of Service (DoS) attack on a remote machine. Affected versions v6.0-rc1 to v6.0-rc3, fixed in v6.0-rc4.	7.5	More Details
CVE-2023-22499	Deno is a runtime for JavaScript and TypeScript that uses V8 and is built in Rust. Multi-threaded programs were able to spoof interactive permission prompt by rewriting the prompt to suggest that program is waiting on user confirmation to unrelated action. A malicious program could clear the terminal screen after permission prompt was shown and write a generic message. This situation impacts users who use Web Worker API and relied on interactive permission prompt. The reproduction is very timing sensitive and can’t be reliably reproduced on every try. This problem can not be exploited on systems that do not attach an interactive prompt (for example headless servers). The problem has been fixed in Deno v1.29.3; it is recommended all users update to this version. Users are advised to upgrade. Users unable to upgrade may run with --no-prompt flag to disable interactive permission prompts.	7.5	More Details
CVE-2022-4499	TP-Link routers, Archer C5 and WR710N-V1, using the latest software, the strcmp function used for checking credentials in httpd, is susceptible to a side-channel attack. By measuring the response time of the httpd process, an attacker could guess each byte of the username and password.	7.5	More Details
CVE-2021-32837	mechanize, a library for automatically interacting with HTTP web servers, contains a regular expression that is vulnerable to regular expression denial of service (ReDoS) prior to version 0.4.6. If a web server responds in a malicious way, then mechanize could crash. Version 0.4.6 has a patch for the issue.	7.5	More Details
CVE-2022-3693	Path Traversal vulnerability in Deytek Informatics FileOrbis File Management System allows Path Traversal.This issue affects FileOrbis File Management System: from unspecified before 10.6.3.	7.5	More Details
CVE-2023-22602	When using Apache Shiro before 1.11.0 together with Spring Boot 2.6+, a specially crafted HTTP request may cause an authentication bypass. The authentication bypass occurs when Shiro and Spring Boot are using different pattern-matching techniques. Both Shiro and Spring Boot < 2.6 default to Ant style pattern matching. Mitigation: Update to Apache Shiro 1.11.0, or set the following Spring Boot configuration value: `spring.mvc.pathmatch.matching-strategy = ant_path_matcher`	7.5	More Details
CVE-2022-41721	A request smuggling attack is possible when using MaxBytesHandler. When using MaxBytesHandler, the body of an HTTP request is not fully consumed. When the server attempts to read HTTP2 frames from the connection, it will instead be reading the body of the HTTP request, which could be attacker-manipulated to represent arbitrary HTTP2 requests.	7.5	More Details
CVE-2023-0158	NLnet Labs Krill supports direct access to the RRDP repository content through its built-in web server at the "/rrdp" endpoint. Prior to 0.12.1 a direct query for any existing directory under "/rrdp/", rather than an RRDP file such as "/rrdp/notification.xml" as would be expected, causes Krill to crash. If the built-in "/rrdp" endpoint is exposed directly to the internet, then malicious remote parties can cause the publication server to crash. The repository content is not affected by this, but the availability of the server and repository can cause issues if this attack is persistent and is not mitigated.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4621	Panasonic Sanyo CCTV Network Cameras versions 1.02-05 and 2.03-0x are vulnerable to CSRFs that can be exploited to allow an attacker to perform changes with administrator level privileges.	7.5	More Details
CVE-2022-40319	The LISTSERV 17 web interface allows remote attackers to conduct Insecure Direct Object References (IDOR) attacks via a modified email address in a wa.exe URL. The impact is unauthorized modification of a victim's LISTSERV account.	7.5	More Details
CVE-2022-47630	Trusted Firmware-A through 2.8 has an out-of-bounds read in the X.509 parser for parsing boot certificates. This affects downstream use of get_ext and auth_nvctr. Attackers might be able to trigger dangerous read side effects or obtain sensitive information about microarchitectural state.	7.4	More Details
CVE-2022-21191	Versions of the package global-modules-path before 3.0.0 are vulnerable to Command Injection due to missing input sanitization or other checks and sandboxes being employed to the getPath function.	7.4	More Details
CVE-2022-3143	wildfly-elytron: possible timing attacks via use of unsafe comparator. A flaw was found in Wildfly-elytron. Wildfly-elytron uses java.util.Arrays.equals in several places, which is unsafe and vulnerable to timing attacks. To compare values securely, use java.security.MessageDigest.isEqual instead. This flaw allows an attacker to access secure information or impersonate an authed user.	7.4	More Details
CVE-2022-46370	Rumpus - FTP server version 9.0.7.1 Improper Token Verification– vulnerability may allow bypassing identity verification.	7.3	More Details
CVE-2023-0324	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file admin/page-login.php. The manipulation of the argument email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-218426 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2023-22480	KubeOperator is an open source Kubernetes distribution focused on helping enterprises plan, deploy and operate production-level K8s clusters. In KubeOperator versions 3.16.3 and below, API interfaces with unauthorized entities and can leak sensitive information. This vulnerability could be used to take over the cluster under certain conditions. This issue has been patched in version 3.16.4.	7.3	More Details
CVE-2023-22478	KubePi is a modern Kubernetes panel. The API interfaces with unauthorized entities and may leak sensitive information. This issue has been patched in version 1.6.4. There are currently no known workarounds.	7.3	More Details
CVE-2023-22947	Insecure folder permissions in the Windows installation path of Shibboleth Service Provider (SP) before 3.4.1 allow an unprivileged local attacker to escalate privileges to SYSTEM via DLL planting in the service executable's folder. This occurs because the installation goes under C:\opt (rather than C:\Program Files) by default. NOTE: the vendor disputes the significance of this report, stating that "We consider the ACLs a best effort thing" and "it was a documentation mistake."	7.3	More Details
CVE-2015-10063	A vulnerability was found in saemorris TheRadSystem and classified as critical. This issue affects the function redirect of the file _login.php. The manipulation of the argument user/pass leads to sql injection. The attack may be initiated remotely. The identifier of the patch is bfba26bd34af31648a11af35a0bb66f1948752a6. It is recommended to apply a patch to fix this issue. The identifier VDB-218453 was assigned to this vulnerability.	7.3	More Details
CVE-2023-0332	A vulnerability was found in SourceCodester Online Food Ordering System 2.0. It has been classified as critical. Affected is an unknown function of the file admin/manage_user.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-218472.	7.3	More Details
CVE-2022-46949	Helmet Store Showroom Site v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Master.php?f=delete_helmet.	7.2	More Details
CVE-2022-46947	Helmet Store Showroom Site v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Master.php?f=delete_category.	7.2	More Details
CVE-2022-46946	Helmet Store Showroom Site v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Master.php?f=delete_brand.	7.2	More Details
CVE-2022-42289	NVIDIA BMC contains a vulnerability in SPX REST API, where an authorized attacker can inject arbitrary shell commands, which may lead to code execution, denial of service, information disclosure and data tampering.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46950	Dynamic Transaction Queuing System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/ajax.php?action=delete_window.	7.2	More Details
CVE-2022-46951	Dynamic Transaction Queuing System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/ajax.php?action=delete_uploads.	7.2	More Details
CVE-2023-22851	Tiki before 24.2 allows lib/importer/tikiimporter_blog_wordpress.php PHP Object Injection by an admin because of an unserialize call.	7.2	More Details
CVE-2022-46952	Dynamic Transaction Queuing System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/ajax.php?action=delete_user.	7.2	More Details
CVE-2022-42278	NVIDIA BMC contains a vulnerability in SPX REST API, where an authorized attacker can read and write to arbitrary locations within the memory context of the IPMI server process, which may lead to code execution, denial of service, information disclosure and data tampering.	7.2	More Details
CVE-2022-42279	NVIDIA BMC contains a vulnerability in SPX REST API, where an authorized attacker can inject arbitrary shell commands, which may lead to code execution, denial of service, information disclosure and data tampering.	7.2	More Details
CVE-2022-4616	The webserver in Delta DX-3021 versions prior to 1.24 is vulnerable to command injection through the network diagnosis page. This vulnerability could allow a remote unauthenticated user to add files, delete files, and change file permissions.	7.2	More Details
CVE-2022-46956	Dynamic Transaction Queuing System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/manage_user.php.	7.2	More Details
CVE-2023-22598	InHand Networks InRouter 302, prior to version IR302 V3.5.56, and InRouter 615, prior to version InRouter6XX-S-V2.3.0.r5542, contain vulnerability CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'). An unauthorized user with privileged access to the local web interface or the cloud account managing the affected devices could push a specially crafted configuration update file to gain root access. This could lead to remote code execution with root privileges.	7.2	More Details
CVE-2022-42290	NVIDIA BMC contains a vulnerability in SPX REST API, where an authorized attacker can inject arbitrary shell commands, which may lead to code execution, denial of service, information disclosure and data tampering.	7.2	More Details
CVE-2022-46953	Dynamic Transaction Queuing System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/ajax.php?action=save_window.	7.2	More Details
CVE-2023-0254	The Simple Membership WP user Import plugin for WordPress is vulnerable to SQL Injection via the ‘orderby’ parameter in versions up to, and including, 1.7 due to insufficient escaping on the user supplied parameter. This makes it possible for authenticated attackers with administrative privileges to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.2	More Details
CVE-2022-46472	Helmet Store Showroom Site v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /hss/classes/Users.php?f=delete.	7.2	More Details
CVE-2022-46372	Alotcer - AR7088H-A firmware version 16.10.3 Command execution Improper validation of unspecified input field may allow Authenticated command execution.	7.2	More Details
CVE-2022-4547	The Conditional Payment Methods for WooCommerce WordPress plugin through 1.0 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by [high privilege users such as adminlusers with a role as low as admin.	7.2	More Details
CVE-2023-22280	MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allow a remote authenticated attacker with an administrative privilege to execute an arbitrary OS command.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26402	Insufficient bounds checking in ASP (AMD Secure Processor) firmware while handling BIOS mailbox commands, may allow an attacker to write partially-controlled data out-of-bounds to SMM or SEV-ES regions which may lead to a potential loss of integrity and availability.	7.1	More Details
CVE-2022-23532	APOC (Awesome Procedures on Cypher) is an add-on library for Neo4j that provides hundreds of procedures and functions. A path traversal vulnerability found in the apoc.export.* procedures of apoc plugins in Neo4j Graph database. The issue allows a malicious actor to potentially break out of the expected directory. The vulnerability is such that files could only be created but not overwritten. For the vulnerability to be exploited, an attacker would need access to execute an arbitrary query, either by having access to an authenticated Neo4j client, or a Cypher injection vulnerability in an application. The minimum versions containing patch for this vulnerability are 4.4.0.12 and 4.3.0.12 and 5.3.1. As a workaround, you can control the allowlist of the procedures that can be used in your system, and/or turn off local file access by setting apoc.export.file.enabled=false.	7.1	More Details
CVE-2021-46779	Insufficient input validation in SVC_ECC_PRIMITIVE system call in a compromised user application or ABL may allow an attacker to corrupt ASP (AMD Secure Processor) OS memory which may lead to potential loss of integrity and availability.	7.1	More Details
CVE-2022-41858	A flaw was found in the Linux kernel. A NULL pointer dereference may occur while a slip driver is in progress to detach in sl_tx_timeout in drivers/net/slip/slip.c. This issue could allow an attacker to crash the system or leak internal kernel information.	7.1	More Details
CVE-2022-42280	NVIDIA BMC contains a vulnerability in SPX REST auth handler, where an un-authorized attacker can exploit a path traversal, which may lead to authentication bypass.	7.1	More Details
CVE-2023-22599	InHand Networks InRouter 302, prior to version IR302 V3.5.56, and InRouter 615, prior to version InRouter6XX-S-V2.3.0.r5542, contain vulnerability CWE-760: Use of a One-way Hash with a Predictable Salt. They send MQTT credentials in response to HTTP/HTTPS requests from the cloud platform. These credentials are encoded using a hardcoded string into an MD5 hash. This string could be easily calculated by an unauthorized user who spoofed sending an HTTP/HTTPS request to the devices. This could result in the affected devices being temporarily disconnected from the cloud platform and allow the user to receive MQTT commands with potentially sensitive information.	7.0	More Details
CVE-2022-46369	Rumpus - FTP server version 9.0.7.1 Persistent cross-site scripting (PXSS) – vulnerability may allow inserting scripts into unspecified input fields.	6.8	More Details
CVE-2022-46368	Rumpus - FTP server version 9.0.7.1 Cross-site request forgery (CSRF) – vulnerability may allow unauthorized action on behalf of authenticated users.	6.8	More Details
CVE-2022-46367	Rumpus - FTP server Cross-site request forgery (CSRF) – Privilege escalation vulnerability that may allow privilege escalation.	6.8	More Details
CVE-2023-22488	Flarum is a forum software for building communities. Using the notifications feature, one can read restricted/private content and bypass access checks that would be in place for such content. The notification-sending component does not check that the subject of the notification can be seen by the receiver, and proceeds to send notifications through their different channels. The alerts do not leak data despite this as they are listed based on a visibility check, however, emails are still sent out. This means that, for extensions which restrict access to posts, any actor can bypass the restriction by subscribing to the discussion if the Subscriptions extension is enabled. The attack allows the leaking of some posts in the forum database, including posts awaiting approval, posts in tags the user has no access to if they could subscribe to a discussion before it becomes private, and posts restricted by third-party extensions. All Flarum versions prior to v1.6.3 are affected. The vulnerability has been fixed and published as flarum/core v1.6.3. All communities running Flarum should upgrade as soon as possible to v1.6.3. As a workaround, disable the Flarum Subscriptions extension or disable email notifications altogether. There are no other supported workarounds for this issue for Flarum versions below 1.6.3.	6.8	More Details
CVE-2022-39187	Rumpus - FTP server version 9.0.7.1 has a Reflected cross-site scripting (RXSS) vulnerability through unspecified vectors.	6.8	More Details
CVE-2022-42281	NVIDIA DGX A100 contains a vulnerability in SBIOS in the FsRecovery, which may allow a highly privileged local attacker to cause an out-of-bounds write, which may lead to code execution, denial of service, compromised integrity, and information disclosure.	6.7	More Details
CVE-2020-36611	Incorrect Default Permissions vulnerability in Hitachi Tuning Manager on Linux (Hitachi Tuning Manager server, Hitachi Tuning Manager - Agent for RAID, Hitachi Tuning Manager - Agent for NAS, Hitachi Tuning Manager - Agent for SAN Switch components) allows local users to read and write specific files.This issue affects Hitachi Tuning Manager: before 8.8.5-00.	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3628	A buffer overflow flaw was found in the Linux kernel Broadcom Full MAC Wi-Fi driver. This issue occurs when a user connects to a malicious USB device. This can allow a local user to crash the system or escalate their privileges.	6.6	More Details
CVE-2022-42282	NVIDIA BMC contains a vulnerability in SPX REST API, where an authorized attacker can access arbitrary files, which may lead to information disclosure.	6.5	More Details
CVE-2023-22414	A Missing Release of Memory after Effective Lifetime vulnerability in Flexible PIC Concentrator (FPC) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker from the same shared physical or logical network, to cause a heap memory leak and leading to FPC crash. On all Junos PTX Series and QFX10000 Series, when specific EVPN VXLAN Multicast packets are processed, an FPC heap memory leak is observed. The FPC memory usage can be monitored using the CLI command "show heap extensive". Following is an example output. ID Base Total(b) Free(b) Used(b) % Name Peak used % -- -------- --------- --------- --------- --- ---------- ---------- 0 37dcf000 3221225472 1694526368 1526699104 47 Kernel 47 1 17dcf000 1048576 1048576 0 0 TOE DMA 0 2 17ecf000 1048576 1048576 0 0 DMA 0 3 17fcf000 534773760 280968336 253805424 47 Packet DMA 47 This issue affects: Juniper Networks Junos OS PTX Series and QFX10000 Series 20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2; 22.2 versions prior to 22.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 20.1R1 on PTX Series and QFX10000 Series.	6.5	More Details
CVE-2022-3437	A heap-based buffer overflow vulnerability was found in Samba within the GSSAPI unwrap_des() and unwrap_des3() routines of Heimdal. The DES and Triple-DES decryption routines in the Heimdal GSSAPI library allow a length-limited write buffer overflow on malloc() allocated memory when presented with a maliciously small packet. This flaw allows a remote user to send specially crafted malicious data to the application, possibly resulting in a denial of service (DoS) attack.	6.5	More Details
CVE-2021-26403	Insufficient checks in SEV may lead to a malicious hypervisor disclosing the launch secret potentially resulting in compromise of VM confidentiality.	6.5	More Details
CVE-2022-39183	Moodle Plugin - SAML Auth may allow Open Redirect through unspecified vectors.	6.5	More Details
CVE-2022-2815	Insecure Storage of Sensitive Information in GitHub repository publify/publify prior to 9.2.10.	6.5	More Details
CVE-2022-3592	A symlink following vulnerability was found in Samba, where a user can create a symbolic link that will make 'smbd' escape the configured share path. This flaw allows a remote user with access to the exported part of the file system under a share via SMB1 unix extensions or NFS to create symlinks to files outside the 'smbd' configured share path and gain access to another restricted server's filesystem.	6.5	More Details
CVE-2023-22316	Hidden functionality vulnerability in PIX-RT100 versions RT100_TEQ_2.1.1_EQ101 and RT100_TEQ_2.1.2_EQ101 allows a network-adjacent attacker to access the product via undocumented Telnet or SSH services.	6.5	More Details
CVE-2022-41861	A flaw was found in freeradius. A malicious RADIUS client or home server can send a malformed abinary attribute which can cause the server to crash.	6.5	More Details
CVE-2022-0553	There is no check to see if slot 0 is being uploaded from the device to the host. When using encrypted images this means the unencrypted firmware can be retrieved easily.	6.5	More Details
CVE-2023-22404	An Out-of-bounds Write vulnerability in the Internet Key Exchange Protocol daemon (iked) of Juniper Networks Junos OS on SRX series and MX with SPC3 allows an authenticated, network-based attacker to cause a Denial of Service (DoS). iked will crash and restart, and the tunnel will not come up when a peer sends a specifically formatted payload during the negotiation. This will impact other IKE negotiations happening at the same time. Continued receipt of this specifically formatted payload will lead to continuous crashing of iked and thereby the inability for any IKE negotiations to take place. Note that this payload is only processed after the authentication has successfully completed. So the issue can only be exploited by an attacker who can successfully authenticate. This issue affects Juniper Networks Junos OS on SRX Series, and MX Series with SPC3: All versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R3-S1; 21.4 versions prior to 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R1-S2, 22.1R2.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48090	Tramyardg hotel-mgmt-system version 2022.4 is vulnerable to SQL Injection via /app/dao/CustomerDAO.php.	6.5	More Details
CVE-2023-0298	Incorrect Authorization in GitHub repository firefly-iii/firefly-iii prior to 5.8.0.	6.5	More Details
CVE-2023-20527	Improper syscall input validation in the ASP Bootloader may allow a privileged attacker to read memory out-of-bounds, potentially leading to a denial-of-service.	6.5	More Details
CVE-2023-20525	Insufficient syscall input validation in the ASP Bootloader may allow a privileged attacker to read memory outside the bounds of a mapped register potentially leading to a denial of service.	6.5	More Details
CVE-2023-23589	The SafeSocks option in Tor before 0.4.7.13 has a logic error in which the unsafe SOCKS4 protocol can be used but not the safe SOCKS4a protocol, aka TROVE-2022-002.	6.5	More Details
CVE-2023-22597	InHand Networks InRouter 302, prior to version IR302 V3.5.56, and InRouter 615, prior to version InRouter6XX-S-V2.3.0.r5542, contain vulnerability CWE-319: Cleartext Transmission of Sensitive Information. They use an unsecured channel to communicate with the cloud platform by default. An unauthorized user could intercept this communication and steal sensitive information such as configuration information and MQTT credentials; this could allow MQTT command injection.	6.5	More Details
CVE-2023-22852	Tiki through 25.0 allows CSRF attacks that are related to tiki-importer.php and tiki-import_sheet.php.	6.5	More Details
CVE-2022-43391	A buffer overflow vulnerability in the parameter of the CGI program in Zyxel NR7101 firmware prior to V1.15(ACCC.3)C0, which could allow an authenticated attacker to cause denial-of-service (DoS) conditions by sending a crafted HTTP request.	6.5	More Details
CVE-2023-22497	Netdata is an open source option for real-time infrastructure monitoring and troubleshooting. Each Netdata Agent has an automatically generated MACHINE GUID. It is generated when the agent first starts and it is saved to disk, so that it will persist across restarts and reboots. Anyone who has access to a Netdata Agent has access to its MACHINE_GUID. Streaming is a feature that allows a Netdata Agent to act as parent for other Netdata Agents (children), offloading children from various functions (increased data retention, ML, health monitoring, etc) that can now be handled by the parent Agent. Configuration is done via `stream.conf`. On the parent side, users configure in `stream.conf` an API key (any random UUID can do) to provide common configuration for all children using this API key and per MACHINE GUID configuration to customize the configuration for each child. The way this was implemented, allowed an attacker to use a valid MACHINE_GUID as an API key. This affects all users who expose their Netdata Agents (children) to non-trusted users and they also expose to the same users Netdata Agent parents that aggregate data from all these children. The problem has been fixed in: Netdata agent v1.37 (stable) and Netdata agent v1.36.0-409 (nightly). As a workaround, do not enable streaming by default. If you have previously enabled this, it can be disabled. Limiting access to the port on the recipient Agent to trusted child connections may mitigate the impact of this vulnerability.	6.5	More Details
CVE-2023-0105	A flaw was found in Keycloak. This flaw allows impersonation and lockout due to the email trust not being handled correctly in Keycloak. An attacker can shadow other users with the same email and lockout or impersonate them.	6.5	More Details
CVE-2022-45439	A pair of spare WiFi credentials is stored in the configuration file of the Zyxel AX7501-B0 firmware prior to V5.17(ABPC.3)C0 in cleartext. An unauthenticated attacker could use the credentials to access the WLAN service if the configuration file has been retrieved from the device by leveraging another known vulnerability.	6.5	More Details
CVE-2023-22395	A Missing Release of Memory after Effective Lifetime vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In an MPLS scenario specific packets destined to an Integrated Routing and Bridging (irb) interface of the device will cause a buffer (mbuf) to leak. Continued receipt of these specific packets will eventually cause a loss of connectivity to and from the device, and requires a reboot to recover. These mbufs can be monitored by using the CLI command 'show system buffers': user@host> show system buffers 783/1497/2280 mbufs in use (current/cache/total) user@host> show system buffers 793/1487/2280 mbufs in use (current/cache/total) <<<<<< mbuf usage increased This issue affects Juniper Networks Junos OS: All versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R3-S9; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R3-S1; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R2.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41956	Autolab is a course management service, initially developed by a team of students at Carnegie Mellon University, that enables instructors to offer autograded programming assignments to their students over the Web. A file disclosure vulnerability was discovered in Autolab's remote handin feature, whereby users are able to hand-in assignments using paths outside their submission directory. Users can then view the submission to view the file's contents. The vulnerability has been patched in version 2.10.0. As a workaround, ensure that the field for the remote handin feature is empty (Edit Assessment > Advanced > Remote handin path), and that you are not running Autolab as `root` (or any user that has write access to `/`). Alternatively, disable the remote handin feature if it is unneeded by replacing the body of `local_submit` in `app/controllers/assessment/handin.rb` with `render(plain: "Feature disabled", status: :bad_request) && return`.	6.5	More Details
CVE-2022-43392	A buffer overflow vulnerability in the parameter of web server in Zyxel NR7101 firmware prior to V1.15(ACCC.3)C0, which could allow an authenticated attacker to cause denial-of-service (DoS) conditions by sending a crafted authorization request.	6.5	More Details
CVE-2022-34335	IBM Sterling Partner Engagement Manager 6.1.2, 6.2.0, and 6.2.1 could allow an authenticated user to exhaust server resources which could lead to a denial of service. IBM X-Force ID: 229705.	6.5	More Details
CVE-2023-22405	An Improper Preservation of Consistency Between Independent Representations of Shared State vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows an adjacent, unauthenticated attacker to cause a Denial of Service (DoS) to device due to out of resources. When a device is configured with "service-provider/SP style" switching, and mac-limiting is configured on an Aggregated Ethernet (ae) interface, and then a PFE is restarted or the device is rebooted, mac-limiting doesn't work anymore. Please note that the issue might not be apparent as traffic will continue to flow through the device although the mac table and respective logs will indicate that mac limit is reached. Functionality can be restored by removing and re-adding the MAC limit configuration. This issue affects Juniper Networks Junos OS on QFX5k Series, EX46xx Series: All versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S1; 21.3 versions prior to 21.3R3 on; 21.4 versions prior to 21.4R3 on; 22.1 versions prior to 22.1R2 on.	6.5	More Details
CVE-2023-22406	A Missing Release of Memory after Effective Lifetime vulnerability in the kernel of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent, unauthenticated attacker to cause a Denial of Service (DoS). In a segment-routing scenario with OSPF as IGP, when a peer interface continuously flaps, next-hop churn will happen and a continuous increase in Routing Protocol Daemon (rpd) memory consumption will be observed. This will eventually lead to an rpd crash and restart when the memory is full. The memory consumption can be monitored using the CLI command "show task memory detail" as shown in the following example: user@host> show task memory detail | match "RT_NEXTHOPS_TEMPLATE|RT_TEMPLATE_BOOK_KEE" RT_NEXTHOPS_TEMPLATE 1008 1024 T 50 51200 50 51200 RT_NEXTHOPS_TEMPLATE 688 768 T 50 38400 50 38400 RT_NEXTHOPS_TEMPLATE 368 384 T 412330 158334720 412330 158334720 RT_TEMPLATE_BOOK_KEE 2064 2560 T 33315 85286400 33315 85286400 user@host> show task memory detail | match "RT_NEXTHOPS_TEMPLATE|RT_TEMPLATE_BOOK_KEE" RT_NEXTHOPS_TEMPLATE 1008 1024 T 50 51200 50 51200 RT_NEXTHOPS_TEMPLATE 688 768 T 50 38400 50 38400 RT_NEXTHOPS_TEMPLATE 368 384 T 419005 160897920 419005 160897920 <=== RT_TEMPLATE_BOOK_KEE 2064 2560 T 39975 102336000 39975 10233600 <=== This issue affects: Juniper Networks Junos OS All versions prior to 19.3R3-S7; 19.4 versions prior to 19.4R2-S8, 19.4R3-S9; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R3-S3; 21.2 versions prior to 21.2R3-S2; 21.3 versions prior to 21.3R3-S1; 21.4 versions prior to 21.4R2-S1, 21.4R3; 22.1 versions prior to 22.1R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S4-EVO; 21.4 versions prior to 21.4R2-S1-EVO, 21.4R3-EVO; 22.1 versions prior to 22.1R2-EVO.	6.5	More Details
CVE-2023-22407	An Incomplete Cleanup vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent, unauthenticated attacker to cause a Denial of Service (DoS). An rpd crash can occur when an MPLS TE tunnel configuration change occurs on a directly connected router. This issue affects: Juniper Networks Junos OS All versions prior to 18.4R2-S7; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2. Juniper Networks Junos OS Evolved All versions prior to 19.2R3-EVO; 19.3 versions prior to 19.3R3-EVO; 19.4 versions prior to 19.4R3-EVO; 20.1 versions prior to 20.1R3-EVO; 20.2 versions prior to 20.2R2-EVO.	6.5	More Details
CVE-2023-0227	Insufficient Session Expiration in GitHub repository pyload/pyload prior to 0.5.0b3.dev36.	6.5	More Details
CVE-2022-4037	An issue has been discovered in GitLab CE/EE affecting all versions before 15.5.7, all versions starting from 15.6 before 15.6.4, all versions starting from 15.7 before 15.7.2. A race condition can lead to verified email forgery and takeover of third-party accounts when using GitLab as an OAuth provider.	6.4	More Details
CVE-2022-42283	NVIDIA BMC contains a vulnerability in IPMI handler, where an authorized attacker can cause a buffer overflow and cause a denial of service or gain code execution.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4345	Infinite loops in the BPv6, OpenFlow, and Kafka protocol dissectors in Wireshark 4.0.0 to 4.0.1 and 3.6.0 to 3.6.9 allows denial of service via packet injection or crafted capture file	6.3	More Details
CVE-2022-4344	Memory exhaustion in the Kafka protocol dissector in Wireshark 4.0.0 to 4.0.1 and 3.6.0 to 3.6.9 allows denial of service via packet injection or crafted capture file	6.3	More Details
CVE-2023-0281	A vulnerability was found in SourceCodester Online Flight Booking Management System. It has been rated as critical. Affected by this issue is some unknown functionality of the file judge_panel.php. The manipulation of the argument subevent_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-218276.	6.3	More Details
CVE-2023-0303	A vulnerability was found in SourceCodester Online Food Ordering System. It has been rated as critical. Affected by this issue is some unknown functionality of the file view_prod.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-218384.	6.3	More Details
CVE-2023-0283	A vulnerability classified as critical has been found in SourceCodester Online Flight Booking Management System. This affects an unknown part of the file review_search.php of the component POST Parameter Handler. The manipulation of the argument txtsearch leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-218277 was assigned to this vulnerability.	6.3	More Details
CVE-2023-0305	A vulnerability classified as critical was found in SourceCodester Online Food Ordering System. This vulnerability affects unknown code of the file admin_class.php of the component Login Module. The manipulation of the argument username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-218386 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-4890	A vulnerability, which was classified as critical, has been found in abhilash1985 PredictApp. This issue affects some unknown processing of the file config/initializers/new_framework_defaults_7_0.rb of the component Cookie Handler. The manipulation leads to deserialization. The attack may be initiated remotely. The patch is named b067372f3ee26fe1b657121f0f41883ff4461a06. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218387.	6.3	More Details
CVE-2023-0243	A vulnerability classified as critical has been found in TuziCMS 2.0.6. This affects the function index of the file App\Manage\Controller\ArticleController.class.php of the component Article Module. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-218151.	6.3	More Details
CVE-2023-0244	A vulnerability classified as critical was found in TuziCMS 2.0.6. This vulnerability affects the function delall of the file \App\Manage\Controller\KefuController.class.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-218152.	6.3	More Details
CVE-2023-0245	A vulnerability, which was classified as critical, has been found in SourceCodester Online Flight Booking Management System. This issue affects some unknown processing of the file add_contestant.php. The manipulation of the argument add_contestant leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-218153 was assigned to this vulnerability.	6.3	More Details
CVE-2023-0256	A vulnerability was found in SourceCodester Online Food Ordering System 2.0. It has been classified as critical. Affected is an unknown function of the file /fos/admin/ajax.php?action=login of the component Login Page. The manipulation of the argument Username leads to sql injection. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-218184.	6.3	More Details
CVE-2013-10011	A vulnerability was found in aeharding classroom-engagement-system and classified as critical. Affected by this issue is some unknown functionality. The manipulation leads to sql injection. The attack may be launched remotely. The name of the patch is 096de5815c7b414e7339f3439522a446098fb73a. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-218156.	6.3	More Details
CVE-2022-40615	IBM Sterling Partner Engagement Manager 6.1, 6.2, and 6.2.1 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 236208.	6.3	More Details
CVE-2023-0304	A vulnerability classified as critical has been found in SourceCodester Online Food Ordering System. This affects an unknown part of the file admin_class.php of the component Signup Module. The manipulation of the argument email leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-218385 was assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42284	NVIDIA BMC stores user passwords in an obfuscated form in a database accessible by the host. This may lead to a credentials exposure.	6.2	More Details
CVE-2022-39186	EXFO - BV-10 Performance Endpoint Unit misconfiguration. System configuration file has misconfigured permissions	6.2	More Details
CVE-2022-38467	Reflected Cross-Site Scripting (XSS) vulnerability in CRM Perks Forms – WordPress Form Builder <= 1.1.0 ver.	6.1	More Details
CVE-2023-22296	Reflected cross-site scripting vulnerability in MAHO-PBX NetDevancer series MAHO-PBX NetDevancer Lite/Uni/Pro/Cloud prior to Ver.1.11.00, MAHO-PBX NetDevancer VSG Lite/Uni prior to Ver.1.11.00, and MAHO-PBX NetDevancer MobileGate Home/Office prior to Ver.1.11.00 allows a remote unauthenticated attacker to inject an arbitrary script.	6.1	More Details
CVE-2022-39195	A cross-site scripting (XSS) vulnerability in the LISTSERV 17 web interface allows remote attackers to inject arbitrary JavaScript or HTML via the c parameter.	6.1	More Details
CVE-2023-0337	Cross-site Scripting (XSS) - Reflected in GitHub repository lirantal/daloradius prior to master-branch.	6.1	More Details
CVE-2023-0338	Cross-site Scripting (XSS) - Reflected in GitHub repository lirantal/daloradius prior to master-branch.	6.1	More Details
CVE-2023-0042	An issue has been discovered in GitLab CE/EE affecting all versions starting from 11.4 prior to 15.5.7, 15.6 prior to 15.6.4, and 15.7 prior to 15.7.2. GitLab Pages allows redirection to arbitrary protocols.	6.1	More Details
CVE-2023-22298	Open redirect vulnerability in pgAdmin 4 versions prior to v6.14 allows a remote unauthenticated attacker to redirect a user to an arbitrary web site and conduct a phishing attack by having a user to access a specially crafted URL.	6.1	More Details
CVE-2023-22958	The Syracom Secure Login plugin before 3.1.1.0 for Jira may allow spoofing of 2FA PIN validation via the plugins/servlet/twofactor/public/pinvalidation target parameter.	6.1	More Details
CVE-2021-46872	An issue was discovered in Nim before 1.6.2. The RST module of the Nim language stdlib, as used in NimForum and other products, permits the javascript: URI scheme and thus can lead to XSS in some applications. (Nim versions 1.6.2 and later are fixed; there may be backports of the fix to some earlier versions. NimForum 2.2.0 is fixed.)	6.1	More Details
CVE-2022-40704	A XSS vulnerability was found in phoromatic_r_add_test_details.php in phoronix-test-suite.	6.1	More Details
CVE-2023-0314	Cross-site Scripting (XSS) - Reflected in GitHub repository thorsten/phpmyfaq prior to 3.1.10.	6.1	More Details
CVE-2022-3904	The MonsterInsights WordPress plugin before 8.9.1 does not sanitize or escape page titles in the top posts/pages section, allowing an unauthenticated attacker to inject arbitrary web scripts into the titles by spoofing requests to google analytics.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22397	An Allocation of Resources Without Limits or Throttling weakness in the memory management of the Packet Forwarding Engine (PFE) on Juniper Networks Junos OS Evolved PTX10003 Series devices allows an adjacently located attacker who has established certain preconditions and knowledge of the environment to send certain specific genuine packets to begin a Time-of-check Time-of-use (TOCTOU) Race Condition attack which will cause a memory leak to begin. Once this condition begins, and as long as the attacker is able to sustain the offending traffic, a Distributed Denial of Service (DDoS) event occurs. As a DDoS event, the offending packets sent by the attacker will continue to flow from one device to another as long as they are received and processed by any devices, ultimately causing a cascading outage to any vulnerable devices. Devices not vulnerable to the memory leak will process and forward the offending packet(s) to neighboring devices. Due to internal anti-flood security controls and mechanisms reaching their maximum limit of response in the worst-case scenario, all affected Junos OS Evolved devices will reboot in as little as 1.5 days. Reboots to restore services cannot be avoided once the memory leak begins. The device will self-recover after crashing and rebooting. Operator intervention isn't required to restart the device. This issue affects: Juniper Networks Junos OS Evolved on PTX10003: All versions prior to 20.4R3-S4-EVO; 21.3 versions prior to 21.3R3-S1-EVO; 21.4 versions prior to 21.4R2-S2-EVO, 21.4R3-EVO; 22.1 versions prior to 22.1R1-S2-EVO, 22.1R2-EVO; 22.2 versions prior to 22.2R2-EVO. To check memory, customers may VTY to the PFE first then execute the following show statement: show jexpr jtm ingress-main-memory chip 255	no-more Alternatively one may execute from the RE CLI: request pfe execute target fpc0 command "show jexpr jtm ingress-main-memory chip 255	no-more" Iteration 1: Example output: Mem type: NH, alloc type: JTM 136776 bytes used (max 138216 bytes used) 911568 bytes available (909312 bytes from free pages) Iteration 2: Example output: Mem type: NH, alloc type: JTM 137288 bytes used (max 138216 bytes used) 911056 bytes available (909312 bytes from free pages) The same can be seen in the CLI below, assuming the scale does not change: show npu memory info Example output: FPC0:NPU16 mem-util-jnh-nh-size 2097152 FPC0:NPU16 mem-util-jnh-nh-allocated 135272 FPC0:NPU16 mem-util-jnh-nh-utilization 6	6.1	More Details
CVE-2022-45728	Doctor Appointment Management System v1.0.0 was discovered to contain a cross-site scripting (XSS) vulnerability.	6.1	More Details
CVE-2022-45729	A cross-site scripting (XSS) vulnerability in Doctor Appointment Management System v1.0.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Employee ID parameter.	6.1	More Details
CVE-2022-46622	A cross-site scripting (XSS) vulnerability in Judging Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the firstname parameter.	6.1	More Details
CVE-2022-4295	The Show All Comments WordPress plugin before 7.0.1 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against a logged in high privilege users such as admin.	6.1	More Details
CVE-2022-4320	The WordPress Events Calendar WordPress plugin before 1.4.5 does not sanitize and escapes a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against both unauthenticated and authenticated users (such as high-privilege ones like admin).	6.1	More Details
CVE-2021-46767	Insufficient input validation in the ASP may allow an attacker with physical access, unauthorized write access to memory potentially leading to a loss of integrity or denial of service.	6.1	More Details
CVE-2023-0312	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.10.	6.1	More Details
CVE-2022-42285	DGX A100 SBIOS contains a vulnerability in the Pre-EFI Initialization (PEI)phase, where a privileged user can disable SPI flash protection, which may lead to denial of service, escalation of privileges, or data tampering.	6.0	More Details
CVE-2022-42286	DGX A100 SBIOS contains a vulnerability in Bds, which may lead to code execution, denial of service, or escalation of privileges.	6.0	More Details
CVE-2022-42287	NVIDIA BMC contains a vulnerability in IPMI handler, where an authorized attacker can upload and download arbitrary files under certain circumstances, which may lead to denial of service, escalation of privileges, information disclosure and data tampering.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22492	ZITADEL is a combination of Auth0 and Keycloak. RefreshTokens is an OAuth 2.0 feature that allows applications to retrieve new access tokens and refresh the user's session without the need for interacting with a UI. RefreshTokens were not invalidated when a user was locked or deactivated. The deactivated or locked user was able to obtain a valid access token only through a refresh token grant. When the locked or deactivated user's session was already terminated ("logged out") then it was not possible to create a new session. Renewal of access token through a refresh token grant is limited to the configured amount of time (RefreshTokenExpiration). As a workaround, ensure the RefreshTokenExpiration in the OIDC settings of your instance is set according to your security requirements. This issue has been patched in versions 2.17.3 and 2.16.4.	5.9	More Details
CVE-2023-22402	A Use After Free vulnerability in the kernel of Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). In a Non Stop Routing (NSR) scenario, an unexpected kernel restart might be observed if "bgp auto-discovery" is enabled and if there is a BGP neighbor flap of auto-discovery sessions for any reason. This is a race condition which is outside of an attackers direct control and it depends on system internal timing whether this issue occurs. This issue affects Juniper Networks Junos OS Evolved: 21.3 versions prior to 21.3R3-EVO; 21.4 versions prior to 21.4R2-EVO; 22.1 versions prior to 22.1R2-EVO; 22.2 versions prior to 22.2R1-S1-EVO, 22.2R2-EVO.	5.9	More Details
CVE-2022-3613	An issue has been discovered in GitLab CE/EE affecting all versions before 15.5.7, all versions starting from 15.6 before 15.6.4, all versions starting from 15.7 before 15.7.2. A crafted Prometheus Server query can cause high resource consumption and may lead to Denial of Service.	5.8	More Details
CVE-2022-2907	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.9 before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2. It was possible to read repository content by an unauthorised user if a project member used a crafted link.	5.7	More Details
CVE-2023-20523	TOCTOU in the ASP may allow a physical attacker to write beyond the buffer bounds, potentially leading to a loss of integrity or denial of service.	5.7	More Details
CVE-2022-2155	A vulnerability exists in the affected versions of Lumada APM's User Asset Group feature due to a flaw in access control mechanism implementation on the "Limited Engineer" role, granting it access to the embedded Power BI reports feature. An attacker that manages to exploit the vulnerability on a customer's Lumada APM could access unauthorized information by gaining unauthorized access to any Power BI reports installed by the customer. Furthermore, the vulnerability enables an attacker to manipulate asset issue comments on assets, which should not be available to the attacker. Affected versions * Lumada APM on-premises version 6.0.0.0 - 6.4.0.* List of CPEs: * cpe:2.3:a:hitachienergy:lumada_apm:6.0.0.0:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:lumada_apm:6.1.0.0:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:lumada_apm:6.2.0.0:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:lumada_apm:6.3.0.0:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:lumada_apm:6.4.0.0:*:*:*:*:*:*:*	5.7	More Details
CVE-2013-10013	A vulnerability was found in Bricco Authenticator Plugin. It has been declared as critical. This vulnerability affects the function authenticate/compare of the file src/java/talentum/escenic/plugins/authenticator/authenticators/DBAuthenticator.java. The manipulation leads to sql injection. Upgrading to version 1.39 is able to address this issue. The name of the patch is a5456633ff75e8f13705974c7ed1ce77f3f142d5. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-218428.	5.5	More Details
CVE-2015-10060	A vulnerability was found in MNBikeways database and classified as critical. This issue affects some unknown processing of the file Data/views.py. The manipulation of the argument id1/id2 leads to sql injection. The identifier of the patch is 829a027aca7c17f5a7ec1addca8dd5d5542f86ac. It is recommended to apply a patch to fix this issue. The identifier VDB-218417 was assigned to this vulnerability.	5.5	More Details
CVE-2015-10061	A vulnerability was found in evandro-machado Trabalho-Web2. It has been classified as critical. This affects an unknown part of the file src/java/br/com/magazine/dao/ClienteDAO.java. The manipulation leads to sql injection. The patch is named f59ac954625d0a4f6d34f069a2e26686a7a20aeb. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218427.	5.5	More Details
CVE-2016-15021	A vulnerability was found in nickzren alsdb. It has been rated as critical. This issue affects some unknown processing. The manipulation leads to sql injection. Upgrading to version v2 is able to address this issue. The identifier of the patch is cbc79a68145e845f951113d184b4de207c341599. It is recommended to upgrade the affected component. The identifier VDB-218429 was assigned to this vulnerability.	5.5	More Details
CVE-2015-10064	A vulnerability was found in VictorFerraresi pokemon-database-php. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. The patch is named dd0e1e6cdf648d6a3deff441f515bcb1d7573d68. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218455.	5.5	More Details
CVE-2021-4313	A vulnerability was found in NethServer phonenehome. It has been rated as critical. This issue affects the function get_info/get_country_coor of the file server/index.php. The manipulation leads to sql injection. The identifier of the patch is 759c30b0ddd7d493836bbdf695cf71624b377391. It is recommended to apply a patch to fix this issue. The identifier VDB-218393 was assigned to this vulnerability.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0316	Path Traversal: '\..\filename' in GitHub repository froxlor/froxlor prior to 2.0.0.	5.5	More Details
CVE-2013-10012	A vulnerability, which was classified as critical, was found in antonbolling clan7ups. Affected is an unknown function of the component Login/Session. The manipulation leads to sql injection. The name of the patch is 25afad571c488291033958d845830ba0a1710764. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-218388.	5.5	More Details
CVE-2016-15020	A vulnerability was found in liftkit database up to 2.13.1. It has been classified as critical. This affects the function processOrderBy of the file src/Query/Query.php. The manipulation leads to sql injection. Upgrading to version 2.13.2 is able to address this issue. The patch is named 42ec8f2b22e0b0b98fb5b4444ed451c1b21d125a. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-218391.	5.5	More Details
CVE-2014-125081	A vulnerability, which was classified as critical, has been found in risheesh debutsav. This issue affects some unknown processing. The manipulation leads to sql injection. The patch is named 7a8430df79277c613449262201cc792db894fc76. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218459.	5.5	More Details
CVE-2015-10065	A vulnerability classified as critical was found in AenBleidd FiND. This vulnerability affects the function init_result of the file validator/my_validator.cpp. The manipulation leads to buffer overflow. The patch is identified as ee2eef34a83644f286c9adcaf30437f92e9c48f1. It is recommended to apply a patch to fix this issue. VDB-218458 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2017-20170	A vulnerability was found in ollpu parontalli. It has been classified as critical. Affected is an unknown function of the file httpdocs/index.php. The manipulation of the argument s leads to sql injection. The patch is identified as 6891bb2dec57dca6daabc15a6d2808c8896620e5. It is recommended to apply a patch to fix this issue. VDB-218418 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2014-125080	A vulnerability has been found in frontaccounting faplanet and classified as critical. This vulnerability affects unknown code. The manipulation leads to path traversal. The patch is identified as a5dcd87f46080a624b1a9ad4b0dd035bbd24ac50. It is recommended to apply a patch to fix this issue. VDB-218398 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2015-10020	A vulnerability has been found in ssn2013 cis450Project and classified as critical. This vulnerability affects the function addUser of the file HeatMapServer/src/com/datformers/servlet/AddAppUser.java. The manipulation leads to sql injection. The name of the patch is 39b495011437a105c7670e17e071f99195b4922e. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-218380.	5.5	More Details
CVE-2014-125077	A vulnerability, which was classified as critical, has been found in pointhi searx_stats. This issue affects some unknown processing of the file cgi/cron.php. The manipulation leads to sql injection. The patch is named 281bd679a4474ddb222d16c1c380f252839cc18f. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218351.	5.5	More Details
CVE-2015-10048	A vulnerability was found in bmattoso desafio_buzz_woody. It has been rated as critical. This issue affects some unknown processing. The manipulation leads to sql injection. The identifier of the patch is cb8220cbae06082c969b1776fcb2fdafb3a1006b. It is recommended to apply a patch to fix this issue. The identifier VDB-218357 was assigned to this vulnerability.	5.5	More Details
CVE-2015-10047	A vulnerability was found in KYUUBI school-register. It has been classified as critical. This affects an unknown part of the file src/DBManager.java. The manipulation leads to sql injection. The patch is named 1cf7e01b878aee923f2b22cc2535c71a680e4c30. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218355.	5.5	More Details
CVE-2015-10046	A vulnerability has been found in lolfeedback and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. The identifier of the patch is 6cf0b5f2228cd8765f734badd37910051000f2b2. It is recommended to apply a patch to fix this issue. The identifier VDB-218353 was assigned to this vulnerability.	5.5	More Details
CVE-2015-10045	A vulnerability, which was classified as critical, was found in tutrantta project_todolist. Affected is the function getAffectedRows/where/insert/update in the library library/Database.php. The manipulation leads to sql injection. The name of the patch is 194a0411bbe11aa4813f13c66b9e8ea403539141. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-218352.	5.5	More Details
CVE-2015-10056	A vulnerability was found in 2071174A vinylmap. It has been classified as critical. Affected is the function contact of the file recordstoreapp/views.py. The manipulation leads to sql injection. The name of the patch is b07b79a1e92cc62574ba0492cce000ef4a7bd25f. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-218400.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2015-10044	A vulnerability classified as critical was found in gophergala sqldump. This vulnerability affects unknown code. The manipulation leads to sql injection. The patch is identified as 76db54e9073b5248b8863e71a63d66a32d567d21. It is recommended to apply a patch to fix this issue. VDB-218350 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2014-125079	A vulnerability was found in agy pontifex.http. It has been declared as critical. This vulnerability affects unknown code of the file lib/Http.coffee. The manipulation leads to sql injection. Upgrading to version 0.1.0 is able to address this issue. The name of the patch is e52a758f96861dcef2dabfecb9da191bb2e07761. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-218356.	5.5	More Details
CVE-2018-25076	A vulnerability classified as critical was found in Events Extension on BigTree. Affected by this vulnerability is the function getRandomFeaturedEventByDate/getUpcomingFeaturedEventsInCategoriesWithSubcategories/recacheEvent/searchResults of the file classes/events.php. The manipulation leads to sql injection. The patch is named 11169e48ab1249109485fdb1e0c9fca3d25ba01d. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218395.	5.5	More Details
CVE-2022-4889	A vulnerability classified as critical was found in visegripped Stracker. Affected by this vulnerability is the function getHistory of the file doc_root/public_html/stracker/api.php. The manipulation of the argument symbol/startDate/endDate leads to sql injection. The identifier of the patch is 63e1b040373ee5b6c7d1e165ecf5ae1603d29e0a. It is recommended to apply a patch to fix this issue. The identifier VDB-218377 was assigned to this vulnerability.	5.5	More Details
CVE-2015-10043	A vulnerability, which was classified as critical, was found in abreen Apollo. This affects an unknown part. The manipulation of the argument file leads to path traversal. The patch is named 6206406630780bbd074aff34f4683fb764faba71. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218307.	5.5	More Details
CVE-2015-10051	A vulnerability, which was classified as critical, has been found in bony2023 Discussion-Board. Affected by this issue is the function display_all_replies of the file functions/main.php. The manipulation of the argument str leads to sql injection. The patch is identified as 26439bc4c63632d63ba89ebc0f149b25a9010361. It is recommended to apply a patch to fix this issue. VDB-218378 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2015-10062	A vulnerability, which was classified as problematic, was found in galaxy-data-resource up to 14.10.0. This affects an unknown part of the component Command Line Template. The manipulation leads to injection. Upgrading to version 14.10.1 is able to address this issue. The patch is named 50d65f45d3f5be5d1fbff2e45ac5cec075f07d42. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-218451.	5.5	More Details
CVE-2016-15018	A vulnerability was found in krail-jpa up to 0.9.1. It has been classified as critical. This affects an unknown part. The manipulation leads to sql injection. Upgrading to version 0.9.2 is able to address this issue. The identifier of the patch is c1e848665492e21ef6cc9be443205e36b9a1f6be. It is recommended to upgrade the affected component. The identifier VDB-218373 was assigned to this vulnerability.	5.5	More Details
CVE-2015-10055	A vulnerability was found in PictureThisWebServer and classified as critical. This issue affects the function router.post of the file routes/user.js. The manipulation of the argument username/password leads to sql injection. The patch is named 68b9dc346e88b494df00d88c7d058e96820e1479. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218399.	5.5	More Details
CVE-2022-4121	In libetpan a null pointer dereference in mailimap_mailbox_data_status_free in low-level/imap/mailimap_types.c was found that could lead to a remote denial of service or other potential consequences.	5.5	More Details
CVE-2015-10054	A vulnerability, which was classified as critical, was found in githuis P2Manage. This affects the function Execute of the file PTwoManage/Database.cs. The manipulation of the argument sql leads to sql injection. The identifier of the patch is 717380aba80002414f82d93c770035198b7858cc. It is recommended to apply a patch to fix this issue. The identifier VDB-218397 was assigned to this vulnerability.	5.5	More Details
CVE-2022-47929	In the Linux kernel before 6.1.6, a NULL pointer dereference bug in the traffic control subsystem allows an unprivileged user to trigger a denial of service (system crash) via a crafted traffic control configuration that is set up with "tc qdisc" and "tc class" commands. This affects qdisc_graft in net/sched/sch_api.c.	5.5	More Details
CVE-2015-10050	A vulnerability was found in brandonfire miRNA_Database_by_PHP_MySql. It has been declared as critical. This vulnerability affects the function __construct/select_single_rna/count_rna of the file inc/model.php. The manipulation leads to sql injection. The patch is identified as 307c5d510841e6142ddcbbdbb93d0e8a0dc3fd6a. It is recommended to apply a patch to fix this issue. VDB-218374 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2015-10053	A vulnerability classified as critical has been found in prodigasistemas curupira up to 0.1.3. Affected is an unknown function of the file app/controllers/curupira/passwords_controller.rb. The manipulation leads to sql injection. Upgrading to version 0.1.4 is able to address this issue. The patch is identified as 93a9a77896bb66c949acb8e64bceafc74bc8c271. It is recommended to upgrade the affected component. VDB-218394 is the identifier assigned to this vulnerability.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-20171	A vulnerability classified as critical has been found in PrivateSky apersistence. This affects an unknown part of the file db/sql/mysqlUtils.js. The manipulation leads to sql injection. The identifier of the patch is 954425f61634b556fe644837a592a5b8fcfca068. It is recommended to apply a patch to fix this issue. The identifier VDB-218457 was assigned to this vulnerability.	5.5	More Details
CVE-2022-4342	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.1 before 15.5.7, all versions starting from 15.6 before 15.6.4, all versions starting from 15.7 before 15.7.2. A malicious Maintainer can leak masked webhook secrets by changing target URL of the webhook.	5.5	More Details
CVE-2015-10037	A vulnerability, which was classified as critical, was found in ACI_Escola. This affects an unknown part. The manipulation leads to sql injection. The identifier of the patch is 34eed1f7b9295d1424912f79989d8aba5de41e9f. It is recommended to apply a patch to fix this issue. The identifier VDB-217965 was assigned to this vulnerability.	5.5	More Details
CVE-2022-4415	A vulnerability was found in systemd. This security flaw can cause a local information leak due to systemd-coredump not respecting the fs.suid_dumpable kernel setting.	5.5	More Details
CVE-2022-24913	Versions of the package com.fasterxml.util:java-merge-sort before 1.1.0 are vulnerable to Insecure Temporary File in the StdTempFileProvider() function in StdTempFileProvider.java, which uses the permissive File.createTempFile() function, exposing temporary file contents.	5.5	More Details
CVE-2021-26343	Insufficient validation in ASP BIOS and DRTM commands may allow malicious supervisor x86 software to disclose the contents of sensitive memory which may result in information disclosure.	5.5	More Details
CVE-2022-47927	An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. When installing with a pre-existing data directory that has weak permissions, the SQLite files are created with file mode 0644, i.e., world readable to local users. These files include credentials data.	5.5	More Details
CVE-2023-23454	cbq_classify in net/sched/sch_cbq.c in the Linux kernel through 6.1.4 allows attackers to cause a denial of service (slab-out-of-bounds read) because of type confusion (non-negative numbers can sometimes indicate a TC_ACT_SHOT condition rather than valid classification results).	5.5	More Details
CVE-2021-26355	Insufficient fencing and checks in System Management Unit (SMU) may result in access to invalid message port registers that could result in a potential denial-of-service.	5.5	More Details
CVE-2017-20168	A vulnerability was found in jfm-so piWallet. It has been rated as critical. Affected by this issue is some unknown functionality of the file api.php. The manipulation of the argument key leads to sql injection. The patch is identified as b420f8c4cbe7f06a34d1b05e90ee5cdfe0aa83bb. It is recommended to apply a patch to fix this issue. VDB-218006 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2021-26404	Improper input validation and bounds checking in SEV firmware may leak scratch buffer bytes leading to potential information disclosure.	5.5	More Details
CVE-2021-26407	A randomly generated Initialization Vector (IV) may lead to a collision of IVs with the same key potentially resulting in information disclosure.	5.5	More Details
CVE-2023-23455	atm_tc_enqueue in net/sched/sch_atm.c in the Linux kernel through 6.1.4 allows attackers to cause a denial of service because of type confusion (non-negative numbers can sometimes indicate a TC_ACT_SHOT condition rather than valid classification results).	5.5	More Details
CVE-2022-4365	An issue has been discovered in GitLab CE/EE affecting all versions starting from 11.8 before 15.5.7, all versions starting from 15.6 before 15.6.4, all versions starting from 15.7 before 15.7.2. A malicious Maintainer can leak the sentry token by changing the configured URL in the Sentry error tracking settings page.	5.5	More Details
CVE-2014-125074	A vulnerability was found in Nayshlok Voyager. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file Voyager/src/models/DatabaseAccess.java. The manipulation leads to sql injection. The identifier of the patch is f1249f438cd8c39e7ef2f6c8f2ab76b239a02fae. It is recommended to apply a patch to fix this issue. The identifier VDB-218005 was assigned to this vulnerability.	5.5	More Details
CVE-2021-46791	Insufficient input validation during parsing of the System Management Mode (SMM) binary may allow a maliciously crafted SMM executable binary to corrupt Dynamic Root of Trust for Measurement (DRTM) user application memory that may result in a potential denial of service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22409	An Unchecked Input for Loop Condition vulnerability in a NAT library of Juniper Networks Junos OS allows a local authenticated attacker with low privileges to cause a Denial of Service (DoS). When an inconsistent "deterministic NAT" configuration is present on an SRX, or MX with SPC3 and then a specific CLI command is issued the SPC will crash and restart. Repeated execution of this command will lead to a sustained DoS. Such a configuration is characterized by the total number of port blocks being greater than the total number of hosts. An example for such configuration is: [services nat source pool TEST-POOL address x.x.x.0/32 to x.x.x.15/32] [services nat source pool TEST-POOL port deterministic block-size 1008] [services nat source pool TEST-POOL port deterministic host address y.y.y.0/24] [services nat source pool TEST-POOL port deterministic include-boundary-addresses] where according to the following calculation: 65536-1024=64512 (number of usable ports per IP address, implicit) 64512/1008=64 (number of port blocks per Nat IP) x.x.x.0/32 to x.x.x.15/32 = 16 (NAT IP addresses available in NAT pool) total port blocks in NAT Pool = 64 blocks per IP * 16 IPs = 1024 Port blocks host address y.y.y.0/24 = 256 hosts (with include-boundary-addresses) If the port block size is configured to be 4032, then the total port blocks are (64512/4032) * 16 = 256 which is equivalent to the total host addresses of 256, and the issue will not be seen. This issue affects Juniper Networks Junos OS on SRX Series, and MX Series with SPC3: All versions prior to 19.4R3-S10; 20.1 version 20.1R1 and later versions; 20.2 versions prior to 20.2R3-S6; 20.3 versions prior to 20.3R3-S6; 20.4 versions prior to 20.4R3-S5; 21.1 versions prior to 21.1R3-S4; 21.2 versions prior to 21.2R3-S3; 21.3 versions prior to 21.3R3-S3; 21.4 versions prior to 21.4R3-S1; 22.1 versions prior to 22.1R2-S2, 22.1R3; 22.2 versions prior to 22.2R2.	5.5	More Details
CVE-2021-46768	Insufficient input validation in SEV firmware may allow an attacker to perform out-of-bounds memory reads within the ASP boot loader, potentially leading to a denial of service.	5.5	More Details
CVE-2022-4543	A flaw named "EntryBleed" was found in the Linux Kernel Page Table Isolation (KPTI). This issue could allow a local attacker to leak KASLR base via prefetch side-channels based on TLB timing for Intel systems.	5.5	More Details
CVE-2021-26346	Failure to validate the integer operand in ASP (AMD Secure Processor) bootloader may allow an attacker to introduce an integer overflow in the L2 directory table in SPI flash resulting in a potential denial of service.	5.5	More Details
CVE-2015-10036	A vulnerability was found in kylebebak dronfelipe. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. The patch is named 87405b74fe651892d79d0dff62ed17a7eaef6a60. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217951.	5.5	More Details
CVE-2014-125075	A vulnerability was found in gmail-servlet and classified as critical. This issue affects the function search of the file src/Model.java. The manipulation leads to sql injection. The identifier of the patch is 5d72753c2e95bb373aa86824939397dc25f679ea. It is recommended to apply a patch to fix this issue. The identifier VDB-218021 was assigned to this vulnerability.	5.5	More Details
CVE-2023-21599	Adobe InCopy versions 18.0 (and earlier), 17.4 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-4842	A flaw NULL Pointer Dereference in the Linux kernel NTFS3 driver function attr_punch_hole() was found. A local user could use this flaw to crash the system.	5.5	More Details
CVE-2022-4457	Due to a misconfiguration in the manifest file of the WARP client for Android, it was possible to a perform a task hijacking attack. An attacker could create a malicious mobile application which could hijack legitimate app and steal potentially sensitive information when installed on the victim's device.	5.5	More Details
CVE-2015-10039	A vulnerability was found in dobos domino. It has been rated as critical. Affected by this issue is some unknown functionality in the library src/Complex.Domino.Lib/Lib/EntityFactory.cs. The manipulation leads to sql injection. Upgrading to version 0.1.5524.38553 is able to address this issue. The name of the patch is 16f039073709a21a76526110d773a6cce0ce753a. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-218024.	5.5	More Details
CVE-2017-20169	A vulnerability, which was classified as critical, has been found in GGGGGGGG ToN-MasterServer. Affected by this issue is some unknown functionality of the file public_html/irc_updater/svr_request_pub.php. The manipulation leads to sql injection. The patch is identified as 3a4c7e6d51bf95760820e3245e06c6e321a7168a. It is recommended to apply a patch to fix this issue. VDB-218306 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2015-10038	A vulnerability was found in nym3r0s pplv2. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. The patch is named 28f8b0550104044da09f04659797487c59f85b00. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218023.	5.5	More Details
CVE-2023-21598	Adobe InCopy versions 18.0 (and earlier), 17.4 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2014-125076	A vulnerability was found in NoxxieNI Criminals. It has been classified as critical. Affected is an unknown function of the file ingame/roulette.php. The manipulation of the argument gambleMoney leads to sql injection. The patch is identified as 0a60b31271d4cbf8babe4be993d2a3a1617f0897. It is recommended to apply a patch to fix this issue. VDB-218022 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2015-10042	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in Dovgalyuk AIBattle. Affected by this vulnerability is the function registerUser of the file site/procedures.php. The manipulation of the argument postLogin leads to sql injection. The identifier of the patch is 448e9880aac18ae7832f8d065e03e46ce0f1d3e3. It is recommended to apply a patch to fix this issue. The identifier VDB-218305 was assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	5.5	More Details
CVE-2023-21592	Adobe InDesign version 18.0 (and earlier), 17.4 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-21591	Adobe InDesign version 18.0 (and earlier), 17.4 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-0295	The Launchpad plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several of its settings parameters in versions up to, and including, 1.0.13 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	5.5	More Details
CVE-2020-36650	A vulnerability, which was classified as critical, was found in IonicaBizau node-gry up to 5.x. This affects an unknown part. The manipulation leads to command injection. Upgrading to version 6.0.0 is able to address this issue. The patch is named 5108446c1e23960d65e8b973f1d9486f9f9dbd6c. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-218019.	5.5	More Details
CVE-2015-10041	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical has been found in Dovgalyuk AIBattle. Affected is the function sendComments of the file site/procedures.php. The manipulation of the argument text leads to sql injection. The name of the patch is e3aa4d0900167641d41cbccf53909229f00381c9. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-218304. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	5.5	More Details
CVE-2022-4478	The Font Awesome WordPress plugin before 4.3.2 does not validate and escapes some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as a contributor to perform Stored Cross-Site Scripting attacks against logged-in admins.	5.4	More Details
CVE-2022-4477	The Smash Balloon Social Post Feed WordPress plugin before 4.1.6 does not validate and escapes some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as a contributor to perform Stored Cross-Site Scripting attacks against logged-in admins.	5.4	More Details
CVE-2022-4476	The Download Manager WordPress plugin before 3.2.62 does not validate and escapes some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as a contributor to perform Stored Cross-Site Scripting attacks against logged-in admins.	5.4	More Details
CVE-2022-4469	The Simple Membership WordPress plugin before 4.2.2 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admin.	5.4	More Details
CVE-2022-4449	The Page scroll to id WordPress plugin before 1.7.6 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.	5.4	More Details
CVE-2022-4465	The WP Video Lightbox WordPress plugin before 1.9.7 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admin.	5.4	More Details
CVE-2022-4464	Themify Portfolio Post WordPress plugin before 1.2.1 does not validate and escapes some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as a contributor to perform Stored Cross-Site Scripting attacks, which could be used against high privileged users such as admin.	5.4	More Details
CVE-2022-4460	The Sidebar Widgets by CodeLights WordPress plugin through 1.4 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as a contributor to perform Stored Cross-Site Scripting attacks, which could be used against high-privilege users such as admins.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4453	The 3D FlipBook WordPress plugin through 1.13.2 does not validate or escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks against high privilege users like administrators.	5.4	More Details
CVE-2022-4451	The Social Sharing WordPress plugin before 3.3.45 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.	5.4	More Details
CVE-2022-4481	The Mesmerize Companion WordPress plugin before 1.6.135 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.	5.4	More Details
CVE-2022-4480	The Click to Chat WordPress plugin before 3.18.1 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.	5.4	More Details
CVE-2022-46503	A cross-site scripting (XSS) vulnerability in the component /admin/register.php of Online Student Enrollment System v1.0 allows attackers to execute arbitrary web scripts via a crafted payload injected into the name parameter.	5.4	More Details
CVE-2022-4482	The Carousel, Slider, Gallery by WP Carousel WordPress plugin before 2.5.3 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.	5.4	More Details
CVE-2022-4483	The Insert Pages WordPress plugin before 3.7.5 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.	5.4	More Details
CVE-2022-4484	The Social Share, Social Login and Social Comments Plugin WordPress plugin before 7.13.44 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.	5.4	More Details
CVE-2022-4486	The Meteor Slides WordPress plugin before 1.5.7 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.	5.4	More Details
CVE-2022-4487	The Easy Accordion WordPress plugin before 2.2.0 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.	5.4	More Details
CVE-2022-4507	The Real Cookie Banner WordPress plugin before 3.4.10 does not validate and escapes some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as a contributor to perform Stored Cross-Site Scripting attacks against logged-in admins.	5.4	More Details
CVE-2022-4508	The ConvertKit WordPress plugin before 2.0.5 does not validate and escapes some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as a contributor to perform Stored Cross-Site Scripting attacks, which could be used against high-privilege users such as admins.	5.4	More Details
CVE-2022-4544	The MashShare WordPress plugin before 3.8.7 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.	5.4	More Details
CVE-2022-4571	The Seriously Simple Podcasting WordPress plugin before 2.19.1 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.	5.4	More Details
CVE-2022-4578	The Video Conferencing with Zoom WordPress plugin before 4.0.10 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.	5.4	More Details
CVE-2022-4648	The Real Testimonials WordPress plugin before 2.6.0 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.	5.4	More Details
CVE-2022-4653	The Greenshift WordPress plugin before 4.8.9 does not validate and escape one of its shortcode attributes, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attack.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4655	The Welcart e-Commerce WordPress plugin before 2.8.9 does not validate and escapes one of its shortcode attributes, which could allow users with a role as low as a contributor to perform a Stored Cross-Site Scripting attack.	5.4	More Details
CVE-2022-3573	An issue has been discovered in GitLab CE/EE affecting all versions starting from 15.4 before 15.5.7, all versions starting from 15.6 before 15.6.4, all versions starting from 15.7 before 15.7.2. Due to the improper filtering of query parameters in the wiki changes page, an attacker can execute arbitrary JavaScript on the self-hosted instances running without strict CSP.	5.4	More Details
CVE-2022-4431	The WOOCS WordPress plugin before 1.3.9.4 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.	5.4	More Details
CVE-2022-4658	The RSSImport WordPress plugin through 4.6.1 does not validate and escape one of its shortcode attributes, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attack.	5.4	More Details
CVE-2023-0306	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.10.	5.4	More Details
CVE-2015-10040	A vulnerability was found in gitlearn. It has been declared as problematic. This vulnerability affects the function getGrade/getOutOf of the file scripts/config.sh of the component Escape Sequence Handler. The manipulation leads to injection. The attack can be initiated remotely. The patch is identified as 3faa5deaa509012069afe75cd03c21bda5050a64. It is recommended to apply a patch to fix this issue. VDB-218302 is the identifier assigned to this vulnerability.	5.4	More Details
CVE-2023-0308	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.10.	5.4	More Details
CVE-2023-0313	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.10.	5.4	More Details
CVE-2023-0289	Cross-site Scripting (XSS) - Stored in GitHub repository craigk5n/webcalendar prior to master.	5.4	More Details
CVE-2022-46438	A cross-site scripting (XSS) vulnerability in the /admin/article_category.php component of DouPHP v1.7 20221118 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the description parameter.	5.4	More Details
CVE-2022-42704	A cross-site scripting (XSS) vulnerability in Employee Service Center (esc) and Service Portal (sp) in ServiceNow Quebec, Rome, and San Diego allows remote attackers to inject arbitrary web script via the Standard Ticket Conversations widget.	5.4	More Details
CVE-2022-41703	A vulnerability in the SQL Alchemy connector of Apache Superset allows an authenticated user with read access to a specific database to add subqueries to the WHERE and HAVING fields referencing tables on the same database that the user should not have access to, despite the user having the feature flag "ALLOW_ADHOC_SUBQUERY" disabled (default value). This issue affects Apache Superset version 1.5.2 and prior versions and version 2.0.0.	5.4	More Details
CVE-2022-43717	Dashboard rendering does not sufficiently sanitize the content of markdown components leading to possible XSS attack vectors that can be performed by authenticated users with create dashboard permissions. This issue affects Apache Superset version 1.5.2 and prior versions and version 2.0.0.	5.4	More Details
CVE-2022-43718	Upload data forms do not correctly render user input leading to possible XSS attack vectors that can be performed by authenticated users with database connection update permissions. This issue affects Apache Superset version 1.5.2 and prior versions and version 2.0.0.	5.4	More Details
CVE-2022-43720	An authenticated attacker with write CSS template permissions can create a record with specific HTML tags that will not get properly escaped by the toast message displayed when a user deletes that specific CSS template record. This issue affects Apache Superset version 1.5.2 and prior versions and version 2.0.0.	5.4	More Details
CVE-2022-43721	An authenticated attacker with update datasets permission could change a dataset link to an untrusted site, users could be redirected to this site when clicking on that specific dataset. This issue affects Apache Superset version 1.5.2 and prior versions and version 2.0.0.	5.4	More Details
CVE-2023-0310	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.10.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48091	Tramyardg hotel-mgmt-system version 2022.4 is vulnerable to Cross Site Scripting (XSS) via process_update_profile.php.	5.4	More Details
CVE-2022-47102	A cross-site scripting (XSS) vulnerability in Student Study Center Management System V 1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the name parameter.	5.4	More Details
CVE-2023-0323	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.5.14.	5.4	More Details
CVE-2023-0301	Cross-site Scripting (XSS) - Stored in GitHub repository alfio-event/alf.io prior to Alf.io 2.0-M4-2301.	5.4	More Details
CVE-2023-0300	Cross-site Scripting (XSS) - Reflected in GitHub repository alfio-event/alf.io prior to 2.0-M4-2301.	5.4	More Details
CVE-2022-43390	A command injection vulnerability in the CGI program of Zyxel NR7101 firmware prior to V1.15(ACCC.3)C0, which could allow an authenticated attacker to execute some OS commands on a vulnerable device by sending a crafted HTTP request.	5.4	More Details
CVE-2023-0309	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.10.	5.4	More Details
CVE-2023-22730	Shopware is an open source commerce platform based on Symfony Framework and Vue js. In affected versions It was possible to put the same line item multiple times in the cart using the AP. The Cart Validators checked the line item's individuality and the user was able to bypass quantity limits in sales. This problem has been fixed with version 6.4.18.1. Users on major versions 6.1, 6.2, and 6.3 may also obtain this fix via a plugin.	5.3	More Details
CVE-2023-22963	The personnummer implementation before 3.0.3 for Dart mishandles numbers in which the last four digits match the ^000[0-9]$ regular expression.	5.3	More Details
CVE-2022-46176	Cargo is a Rust package manager. The Rust Security Response WG was notified that Cargo did not perform SSH host key verification when cloning indexes and dependencies via SSH. An attacker could exploit this to perform man-in-the-middle (MITM) attacks. This vulnerability has been assigned CVE-2022-46176. All Rust versions containing Cargo before 1.66.1 are vulnerable. Note that even if you don't explicitly use SSH for alternate registry indexes or crate dependencies, you might be affected by this vulnerability if you have configured git to replace HTTPS connections to GitHub with SSH (through git's [`url.<base>.insteadOf`][1] setting), as that'd cause you to clone the crates.io index through SSH. Rust 1.66.1 will ensure Cargo checks the SSH host key and abort the connection if the server's public key is not already trusted. We recommend everyone to upgrade as soon as possible.	5.3	More Details
CVE-2023-0296	The Birthday attack against 64-bit block ciphers flaw (CVE-2016-2183) was reported for the health checks port (9979) on etcd grpc-proxy component. Even though the CVE-2016-2183 has been fixed in the etcd components, to enable periodic health checks from kubelet, it was necessary to open up a new port (9979) on etcd grpc-proxy, hence this port might be considered as still vulnerable to the same type of vulnerability. The health checks on etcd grpc-proxy do not contain sensitive data (only metrics data), therefore the potential impact related to this vulnerability is minimal. The CVE-2023-0296 has been assigned to this issue to track the permanent fix in the etcd component.	5.3	More Details
CVE-2022-3870	An issue has been discovered in GitLab CE/EE affecting all versions starting from 10.0 before 15.5.7, all versions starting from 15.6 before 15.6.4, all versions starting from 15.7 before 15.7.2. GitLab allows unauthenticated users to download user avatars using the victim's user ID, on private instances that restrict public level visibility.	5.3	More Details
CVE-2022-3341	A null pointer dereference issue was discovered in 'FFmpeg' in decode_main_header() function of libavformat/nutdec.c file. The flaw occurs because the function lacks check of the return value of avformat_new_stream() and triggers the null pointer dereference error, causing an application to crash.	5.3	More Details
CVE-2023-20532	Insufficient input validation in the SMU may allow an attacker to improperly lock resources, potentially resulting in a denial of service.	5.3	More Details
CVE-2023-22278	m-FILTER prior to Ver.5.70R01 (Ver.5 Series) and m-FILTER prior to Ver.4.87R04 (Ver.4 Series) allows a remote unauthenticated attacker to bypass authentication and send users' unintended email when email is being sent under the certain conditions. The attacks exploiting this vulnerability have been observed.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4167	Incorrect Authorization check affecting all versions of GitLab EE from 13.11 prior to 15.5.7, 15.6 prior to 15.6.4, and 15.7 prior to 15.7.2 allows group access tokens to continue working even after the group owner loses the ability to revoke them.	5.3	More Details
CVE-2022-46371	Alotcer - AR7088H-A firmware version 16.10.3 Information disclosure. Unspecified error message contains the default administrator user name.	5.3	More Details
CVE-2022-23814	Failure to validate addresses provided by software to BIOS commands may result in a potential loss of integrity of guest memory in a confidential compute environment.	5.3	More Details
CVE-2023-23456	A heap-based buffer overflow issue was discovered in UPX in PackTmt::pack() in p_tmt.cpp file. The flow allows an attacker to cause a denial of service (abort) via a crafted file.	5.3	More Details
CVE-2022-45438	When explicitly enabling the feature flag DASHBOARD_CACHE (disabled by default), the system allowed for an unauthenticated user to access dashboard configuration metadata using a REST API Get endpoint. This issue affects Apache Superset version 1.5.2 and prior versions and version 2.0.0.	5.3	More Details
CVE-2023-23457	A Segmentation fault was found in UPX in PackLinuxElf64::invert_pt_dynamic() in p_lx_elf.cpp. An attacker with a crafted input file allows invalid memory address access that could lead to a denial of service.	5.3	More Details
CVE-2023-22398	An Access of Uninitialized Pointer vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). When an MPLS ping is performed on BGP LSPs, the RPD might crash. Repeated execution of this operation will lead to a sustained DoS. This issue affects: Juniper Networks Junos OS: 15.1 versions prior to 15.1R7-S12; 19.1 versions prior to 19.1R3-S9; 19.2 versions prior to 19.2R1-S9, 19.2R3-S5; 19.3 versions prior to 19.3R3-S6; 19.4 versions prior to 19.4R2-S7, 19.4R3-S8; 20.1 versions prior to 20.1R3-S4; 20.2 versions prior to 20.2R3-S5; 20.3 versions prior to 20.3R3-S5; 20.4 versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R1-S1, 21.1R2; Juniper Networks Junos OS Evolved: All versions prior to 20.4R3-S4; 21.1 versions prior to 21.1R2-EVO.	5.3	More Details
CVE-2022-48257	In Eternal Terminal 6.2.1, etserver and etclient have predictable logfile names in /tmp.	5.3	More Details
CVE-2022-48258	In Eternal Terminal 6.2.1, etserver and etclient have world-readable logfiles.	5.3	More Details
CVE-2022-37436	Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.	5.3	More Details
CVE-2022-42288	NVIDIA BMC contains a vulnerability in IPMI handler, where an unauthorized attacker can use certain oracles to guess a valid BMC username, which may lead to an information disclosure.	5.3	More Details
CVE-2022-23813	The software interfaces to ASP and SMU may not enforce the SNP memory security policy resulting in a potential loss of integrity of guest memory in a confidential compute environment.	5.3	More Details
CVE-2022-23538	github.com/sylabs/scs-library-client is the Go client for the Singularity Container Services (SCS) Container Library Service. When the scs-library-client is used to pull a container image, with authentication, the HTTP Authorization header sent by the client to the library service may be incorrectly leaked to an S3 backing storage provider. This occurs in a specific flow, where the library service redirects the client to a backing S3 storage server, to perform a multi-part concurrent download. Depending on site configuration, the S3 service may be provided by a third party. An attacker with access to the S3 service may be able to extract user credentials, allowing them to impersonate the user. The vulnerable multi-part concurrent download flow, with redirect to S3, is only used when communicating with a Singularity Enterprise 1.x installation, or third party server implementing this flow. Interaction with Singularity Enterprise 2.x, and Singularity Container Services (cloud.sylabs.io), does not trigger the vulnerable flow. We encourage all users to update. Users who interact with a Singularity Enterprise 1.x installation, using a 3rd party S3 storage service, are advised to revoke and recreate their authentication tokens within Singularity Enterprise. There is no workaround available at this time.	5.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4885	A vulnerability has been found in sviehb jefferson up to 0.3 and classified as critical. This vulnerability affects unknown code of the file src/scripts/jefferson. The manipulation leads to path traversal. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. Upgrading to version 0.4 is able to address this issue. The name of the patch is 53b3f2fc34af0bb32afbcee29d18213e61471d87. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-218020.	5.0	More Details
CVE-2022-39182	H C Mingham-Smith Ltd - Tardis 2000 Privilege escalation.Version 1.6 is vulnerable to privilege escalation which may allow a malicious actor to gain system privileges.	4.9	More Details
CVE-2022-4330	The WP Attachments WordPress plugin before 5.0.6 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2022-42462	Auth. Stored Cross-Site Scripting (XSS) vulnerability in Adeel Ahmed's IP Blacklist Cloud plugin <= 5.00 versions.	4.8	More Details
CVE-2022-4442	The Custom Post Types and Custom Fields creator WordPress plugin before 2.3.3 does not sanitize and escape some of its settings, which could allow high-privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example, in multisite setup).	4.8	More Details
CVE-2022-2658	The WP Spell Check WordPress plugin before 9.13 does not escape ignored words, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-4299	The Metricool WordPress plugin before 1.18 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2022-4199	The Link Library WordPress plugin before 7.4.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2022-2251	Improper sanitization of branch names in GitLab Runner affecting all versions prior to 15.3.5, 15.4 prior to 15.4.4, and 15.5 prior to 15.5.2 allows a user who creates a branch with a specially crafted name and gets another user to trigger a pipeline to execute commands in the runner as that other user.	4.8	More Details
CVE-2022-3145	An open redirect vulnerability exists in Okta OIDC Middleware prior to version 5.0.0 allowing an attacker to redirect a user to an arbitrary URL.	4.7	More Details
CVE-2023-0257	A vulnerability was found in SourceCodester Online Food Ordering System 2.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /fos/admin/index.php?page=menu of the component Menu Form. The manipulation of the argument Image with the input <?php system($_GET['c']); ?> leads to unrestricted upload. The attack can be launched remotely. The identifier VDB-218185 was assigned to this vulnerability.	4.7	More Details
CVE-2021-36647	Use of a Broken or Risky Cryptographic Algorithm in the function mbedtls_mpi_exp_mod() in lignum.c in Mbed TLS Mbed TLS all versions before 3.0.0, 2.27.0 or 2.16.11 allows attackers with access to precise enough timing and memory access information (typically an untrusted operating system attacking a secure enclave such as SGX or the TrustZone secure world) to recover the private keys used in RSA.	4.7	More Details
CVE-2021-46795	A TOCTOU (time-of-check to time-of-use) vulnerability exists where an attacker may use a compromised BIOS to cause the TEE OS to read memory out of bounds that could potentially result in a denial of service.	4.7	More Details
CVE-2015-10052	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as problematic, was found in calesanz gibb-modul-151. This affects the function bearbeiten/login. The manipulation leads to open redirect. It is possible to initiate the attack remotely. The patch is named 88a517dc19443081210c804b655e72770727540d. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218379. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	4.6	More Details
CVE-2018-25075	A vulnerability classified as critical has been found in karsany OBridge up to 1.3. Affected is the function getAllStandaloneProcedureAndFunction of the file obridge-main/src/main/java/org/obridge/dao/ProcedureDao.java. The manipulation leads to sql injection. The complexity of an attack is rather high. The exploitability is told to be difficult. Upgrading to version 1.4 is able to address this issue. The name of the patch is 52eca4ad05f3c292aed3178b2f58977686ffa376. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-218376.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2015-10057	A vulnerability was found in Little Apps Little Software Stats. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file inc/class.securelogin.php of the component Password Reset Handler. The manipulation leads to improper access controls. The complexity of an attack is rather high. The exploitation appears to be difficult. Upgrading to version 0.2 is able to address this issue. The identifier of the patch is 07ba8273a9311d1383f3686ac7cb32f20770ab1e. It is recommended to upgrade the affected component. The identifier VDB-218401 was assigned to this vulnerability.	4.6	More Details
CVE-2021-26328	Failure to verify the mode of CPU execution at the time of SNP_INIT may lead to a potential loss of memory integrity for SNP guests.	4.4	More Details
CVE-2022-45440	A vulnerability exists in the FTP server of the Zyxel AX7501-B0 firmware prior to V5.17(ABPC.3)C0, which processes symbolic links on external storage media. A local authenticated attacker with administrator privileges could abuse this vulnerability to access the root file system by creating a symbolic link on external storage media, such as a USB flash drive, and then logging into the FTP server on a vulnerable device.	4.4	More Details
CVE-2021-26396	Insufficient validation of address mapping to IO in ASP (AMD Secure Processor) may result in a loss of memory integrity in the SNP guest.	4.4	More Details
CVE-2023-0221	Product security bypass vulnerability in ACC prior to version 8.3.4 allows a locally logged-in attacker with administrator privileges to bypass the execution controls provided by ACC using the utilman program.	4.4	More Details
CVE-2022-3514	An issue has been discovered in GitLab CE/EE affecting all versions starting from 6.6 before 15.5.7, all versions starting from 15.6 before 15.6.4, all versions starting from 15.7 before 15.7.2. An attacker may cause Denial of Service on a GitLab instance by exploiting a regex issue in the submodule URL parser.	4.3	More Details
CVE-2023-22734	Shopware is an open source commerce platform based on Symfony Framework and Vue js. The newsletter double opt-in validation was not checked properly, and it was possible to skip the complete double opt in process. As a result operators may have inconsistencies in their newsletter systems. This problem has been fixed with version 6.4.18.1. Users are advised to upgrade. Users unable to upgrade may find security measures are available via a plugin for major versions 6.1, 6.2, and 6.3. Users may also disable newsletter registration completely.	4.3	More Details
CVE-2022-4131	An issue has been discovered in GitLab CE/EE affecting all versions starting from 10.8 before 15.5.7, all versions starting from 15.6 before 15.6.4, all versions starting from 15.7 before 15.7.2. An attacker may cause Denial of Service on a GitLab instance by exploiting a regex issue in how the application parses user agents.	4.3	More Details
CVE-2013-10010	A vulnerability classified as problematic has been found in zerochplus. This affects the function PrintResList of the file test/mordor/thread.res.pl. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The patch is named 9ddf9ecca8565341d8d26a3b2f64540bde4fa273. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218007.	4.3	More Details
CVE-2018-14628	An information leak vulnerability was discovered in Samba's LDAP server. Due to missing access control checks, an authenticated but unprivileged attacker could discover the names and preserved attributes of deleted objects in the LDAP store.	4.3	More Details
CVE-2023-22945	In the GrowthExperiments extension for MediaWiki through 1.39, the growthmanagementorlist API allows blocked users (blocked in ApiManageMentorList) to enroll as mentors or edit any of their mentorship-related properties.	4.3	More Details
CVE-2023-0293	The Mediamatic – Media Library Folders plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on its AJAX actions in versions up to, and including, 2.8.1. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to change image categories, which it uses to arrange them in folder views.	4.3	More Details
CVE-2022-4549	The Tickera WordPress plugin before 3.5.1.0 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged-in admin change them via a CSRF attack.	4.3	More Details
CVE-2022-45353	Broken Access Control in Betheme theme <= 26.6.1 on WordPress.	4.3	More Details
CVE-2016-15019	A vulnerability was found in tombh jekbox. It has been rated as problematic. This issue affects some unknown processing of the file lib/server.rb. The manipulation leads to exposure of information through directory listing. The attack may be initiated remotely. The patch is named 64eb2677671018fc08b96718b81e3dbc83693190. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218375.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30544	Cross-Site Request Forgery (CSRF) in MiKa's OSM – OpenStreetMap plugin <= 6.0.1 versions.	4.3	More Details
CVE-2023-0091	A flaw was found in Keycloak, where it did not properly check client tokens for possible revocation in its client credential flow. This flaw allows an attacker to access or modify potentially sensitive information.	3.8	More Details
CVE-2023-22732	Shopware is an open source commerce platform based on Symfony Framework and Vue js. The Administration session expiration was set to one week, when an attacker has stolen the session cookie they could use it for a long period of time. In version 6.4.18.1 an automatic logout into the Administration session has been added. As a result the user will be logged out when they are inactive. Users are advised to upgrade. There are no known workarounds for this issue.	3.7	More Details
CVE-2020-36649	A vulnerability was found in mholt PapaParse up to 5.1.x. It has been classified as problematic. Affected is an unknown function of the file papaparse.js. The manipulation leads to inefficient regular expression complexity. Upgrading to version 5.2.0 is able to address this issue. The name of the patch is 235a12758cd77266d2e98fd715f53536b34ad621. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-218004.	3.5	More Details
CVE-2022-4891	A vulnerability has been found in Sisimai up to 4.25.14p11 and classified as problematic. This vulnerability affects the function to_plain of the file lib/sisimai/string.rb. The manipulation leads to inefficient regular expression complexity. The exploit has been disclosed to the public and may be used. Upgrading to version 4.25.14p12 is able to address this issue. The name of the patch is 51fe2e6521c9c02b421b383943dc9e4bbbe65d4e. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-218452.	3.5	More Details
CVE-2023-0246	A vulnerability, which was classified as problematic, was found in earclink ESPCMS P8.21120101. Affected is an unknown function of the component Content Handler. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-218154 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2018-25074	A vulnerability was found in Prestaul skeemas and classified as problematic. This issue affects some unknown processing of the file validators/base.js. The manipulation of the argument uri leads to inefficient regular expression complexity. The patch is named 65e94eda62dc8dc148ab3e59aa2ccc086ac448fd. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218003.	3.5	More Details
CVE-2015-10059	A vulnerability has been found in s134328 Webapplication-Veganguide and classified as problematic. This vulnerability affects unknown code of the file p05-integration/app/shared/api/apiService.js. The manipulation of the argument country/city leads to cross site scripting. The attack can be initiated remotely. The name of the patch is 2aa760fa4e779e40a28206a32ac22ac10356f519. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-218416.	3.5	More Details
CVE-2023-0327	A vulnerability was found in saemorris TheRadSystem. It has been classified as problematic. Affected is an unknown function of the file users.php. The manipulation of the argument q leads to cross site scripting. It is possible to launch the attack remotely. VDB-218454 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2018-25073	A vulnerability has been found in Newcomer1989 TSN-Ranksystem up to 1.2.6 and classified as problematic. This vulnerability affects the function getlog of the file webinterface/bot.php. The manipulation leads to cross site scripting. The attack can be initiated remotely. Upgrading to version 1.2.7 is able to address this issue. The patch is identified as b3a3cd8efe2cd3bd3c5b3b7abf2fe80dbee51b77. It is recommended to upgrade the affected component. VDB-218002 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2012-10005	A vulnerability has been found in manikandan170890 php-form-builder-class and classified as problematic. Affected by this vulnerability is an unknown functionality of the file PFBC/Element/Textarea.php of the component Textarea Handler. The manipulation of the argument value leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The patch is named 74897993818d826595fd5857038e6703456a594a. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218155.	3.5	More Details
CVE-2023-22471	Deck is a kanban style organization tool aimed at personal planning and project organization for teams integrated with Nextcloud. Broken access control allows a user to delete attachments of other users. There are currently no known workarounds. It is recommended that the Nextcloud Deck app is upgraded to 1.6.5 or 1.7.3 or 1.8.2.	3.5	More Details
CVE-2023-0287	A vulnerability was found in ityouknow favorites-web. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Comment Handler. The manipulation leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-218294 is the identifier assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2015-10049	A vulnerability was found in Overdrive Eletrônica course-builder up to 1.7.x and classified as problematic. Affected by this issue is some unknown functionality of the file coursebuilder/modules/oeditor/oeditor.html. The manipulation leads to cross site scripting. The attack may be launched remotely. Upgrading to version 1.8.0 is able to address this issue. The name of the patch is e39645fd714adb7e549908780235911ae282b21b. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-218372.	3.5	More Details
CVE-2015-10058	A vulnerability, which was classified as problematic, was found in Wikisource Category Browser. This affects an unknown part of the file index.php. The manipulation of the argument lang leads to cross site scripting. It is possible to initiate the attack remotely. The patch is named 764f4e8ce3f9242637df77530c70ae8a2ec4b6a1. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218415.	3.5	More Details
CVE-2023-22489	Flarum is a discussion platform for websites. If the first post of a discussion is permanently deleted but the discussion stays visible, any actor who can view the discussion is able to create a new reply via the REST API, no matter the reply permission or lock status. This includes users that don't have a validated email. Guests cannot successfully create a reply because the API will fail with a 500 error when the user ID 0 is inserted into the database. This happens because when the first post of a discussion is permanently deleted, the `first_post_id` attribute of the discussion becomes `null` which causes access control to be skipped for all new replies. Flarum automatically makes discussions with zero comments invisible so an additional condition for this vulnerability is that the discussion must have at least one approved reply so that `discussions.comment_count` is still above zero after the post deletion. This can open the discussion to uncontrolled spam or just unintentional replies if users still had their tab open before the vulnerable discussion was locked and then post a reply when they shouldn't be able to. In combination with the email notification settings, this could also be used as a way to send unsolicited emails. Versions between `v1.3.0` and `v1.6.3` are impacted. The vulnerability has been fixed and published as flarum/core v1.6.3. All communities running Flarum should upgrade as soon as possible. There are no known workarounds.	3.5	More Details
CVE-2009-10001	A vulnerability classified as problematic was found in jianlinwei cool-php-captcha up to 0.2. This vulnerability affects unknown code of the file example-form.php. The manipulation of the argument captcha with the input %3Cscript%3Ealert(1)%3C/script%3E leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 0.3 is able to address this issue. The name of the patch is c84fb6b153bebaf228feee0cbf50728d27ae3f80. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-218296.	3.5	More Details
CVE-2023-22470	Nextcloud Deck is a kanban style organization tool aimed at personal planning and project organization for teams integrated with Nextcloud. A database error can be generated potentially causing a DoS when performed multiple times. There are currently no known workarounds. It is recommended that the Nextcloud Server is upgraded to 1.6.5 or 1.7.3 or 1.8.2.	3.5	More Details
CVE-2010-10008	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in simplesamlphp simplesamlphp-module-openidprovider up to 0.8.x. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file templates/trust.tpl.php. The manipulation of the argument StateID leads to cross site scripting. The attack can be launched remotely. Upgrading to version 0.9.0 is able to address this issue. The identifier of the patch is 8365d48c863cf06ccf1465cc0a161cefae29d69d. It is recommended to upgrade the affected component. The identifier VDB-218473 was assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	3.5	More Details
CVE-2009-10002	A vulnerability, which was classified as problematic, has been found in dpup fittr-flickr. This issue affects some unknown processing of the file fittr-flickr/features/easy-exif.js of the component EXIF Preview Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The identifier of the patch is 08875dd8a2e5d0d16568bb0d67cb4328062fccde. It is recommended to apply a patch to fix this issue. The identifier VDB-218297 was assigned to this vulnerability.	3.5	More Details
CVE-2017-20167	A vulnerability, which was classified as problematic, was found in Minichan. This affects an unknown part of the file reports.php. The manipulation of the argument headline leads to cross site scripting. It is possible to initiate the attack remotely. The identifier of the patch is fc0e732e58630cba318d6bf49d1388a7aa9d390e. It is recommended to apply a patch to fix this issue. The identifier VDB-217785 was assigned to this vulnerability.	3.5	More Details
CVE-2012-10004	A vulnerability was found in backdrop-contrib Basic Cart on Drupal. It has been classified as problematic. Affected is the function basic_cart_checkout_form_submit of the file basic_cart.cart.inc. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 1.x-1.1.1 is able to address this issue. The patch is identified as a10424ccd4b3b4b433cf33b73c1ad608b11890b4. It is recommended to upgrade the affected component. VDB-217950 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2014-125078	A vulnerability was found in yanheven console and classified as problematic. Affected by this issue is some unknown functionality of the file horizon/static/horizon/js/horizon.instances.js. The manipulation leads to cross site scripting. The attack may be launched remotely. The patch is identified as 32a7b713468161282f2ea01d5e2faff980d924cd. It is recommended to apply a patch to fix this issue. VDB-218354 is the identifier assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4312	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as problematic has been found in Th3-822 Rapidleech. This affects the function zip_go of the file classes/options/zip.php. The manipulation of the argument archive leads to cross site scripting. It is possible to initiate the attack remotely. The patch is named 885a87ea4ee5e14fa95801eca255604fb2e138c6. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218295. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	3.5	More Details
CVE-2022-4309	The Subscribe2 WordPress plugin before 10.38 does not have CSRF check when deleting users, which could allow attackers to make a logged in admin delete arbitrary users by knowing their email via a CSRF attack.	3.1	More Details
CVE-2023-22733	Shopware is an open source commerce platform based on Symfony Framework and Vue js. In affected versions the log module would write out all kind of sent mails. An attacker with access to either the local system logs or a centralized logging store may have access to other users accounts. This issue has been addressed in version 6.4.18.1. For older versions of 6.1, 6.2, and 6.3, corresponding security measures are also available via a plugin. For the full range of functions, we recommend updating to the latest Shopware version. Users unable to upgrade may remove from all users the log module ACL rights or disable logging.	2.7	More Details
CVE-2023-0258	A vulnerability was found in SourceCodester Online Food Ordering System 2.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Category List Handler. The manipulation of the argument Reason with the input "><script>prompt(1)</script> leads to cross site scripting. The attack may be launched remotely. VDB-218186 is the identifier assigned to this vulnerability.	2.4	More Details
CVE-2023-20528	Insufficient input validation in the SMU may allow a physical attacker to exfiltrate SMU memory contents over the I2C bus potentially leading to a loss of confidentiality.	2.4	More Details
CVE-2023-22494	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2016-20018. Reason: This candidate is a reservation duplicate of CVE-2016-20018. Notes: All CVE users should reference CVE-2016-20018 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2022-45148	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-4327	Rejected reason: This issue does not bear any security risk as it's only exploitable by users with administrator or super-administrator roles, who can already do what they want on their site.	N/A	More Details
CVE-2010-10005	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: It is a duplicate of CVE-2010-2799.	N/A	More Details
CVE-2023-0235	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-0237	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-40272	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-0161	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-22885	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-0269	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40271	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-40270	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-3117	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-27676	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-27675	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-23832	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-23827	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-23816	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-46799	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-41812	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2022. Notes: none.	N/A	More Details
CVE-2022-41811	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2022. Notes: none.	N/A	More Details
CVE-2022-41810	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2022. Notes: none.	N/A	More Details
CVE-2022-41809	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2022. Notes: none.	N/A	More Details
CVE-2021-46796	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-46793	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-46761	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-26405	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26399	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-26385	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-26374	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-26358	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-26357	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-26319	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-40273	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-38287	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details