Severity

Medium

Analysis Summary

CVE-2022-25622 CVSS: 5.3

Siemens SIMATIC devices and Siemens SIMIT Simulation Platform are vulnerable to a denial of service, caused by uncontrolled resource consumption in the PROFINET (PNIO) stack when integrated with the Interniche IP stack. By sending specially-crafted TCP segments, a remote attacker could exploit this vulnerability to cause a denial of service.

CVE-2022-25650 CVSS: 3.1

Siemens Mendix Applications could allow a remote authenticated attacker to obtain sensitive information, caused by improper access control when querying the database. By sorting the results using a protected field, an attacker could exploit this vulnerability to obtain the contents of a protected field.

CVE-2022-25751 CVSS: 8.2

Siemens SCALANCE X-300 series is vulnerable to a denial of service, caused by improper validation of the HTTP headers of incoming requests. A remote attacker could exploit this vulnerability to cause the device to crash.

CVE-2022-25752 CVSS: 8.8

Siemens SCALANCE X-300 series could allow a remote attacker to hijack a user's session, caused by the use of insufficiently random values in the webserver when calculating session ids and nonces. An attacker could exploit this vulnerability to gain access to brute-force session ids and hijack existing sessions.

CVE-2022-27194 CVSS: 7.5

Siemens SIMATIC PCS neo, SINETPLAN, and TIA Portal are vulnerable to a denial of service, caused by improper validation of user requests sent to port 8888. By sending specially-crafted packets, a remote attacker could exploit this vulnerability to cause a denial of service.

CVE-2022-27241 CVSS: 5.3

Siemens Mendix applications could allow a remote attacker to obtain sensitive information, caused by the exposure of the internal project structure. By sending a specially crafted request, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.

CVE-2022-27480 CVSS: 5.3

Siemens SICAM A8000 CP-8050 and CP-8031 devices could allow a remote attacker to obtain sensitive information, caused by missing authorization. By sending a specially crafted request, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.

CVE-2022-27481 CVSS: 7.4

Siemens SCALANCE W-1700 (11ac) family devices are vulnerable to a denial of service, caused by a race condition. By sending a specially-crafted ARP request, a remote attacker could exploit this vulnerability to cause a denial of service.

CVE-2022-28328 CVSS: 7.4

Siemens SCALANCE W-1700 (11ac) family devices is vulnerable to a denial of service, caused by improper validation of Multicast LLC frames. By sending a specially-crafted request, a remote attacker could exploit this vulnerability to cause a denial of service.

CVE-2022-28329 CVSS: 4.3

Siemens SCALANCE W-1700 (11ac) family devices is vulnerable to a denial of service, caused by improper validation of user requests by the RemoteCapture feature. By sending a specially-crafted request, a remote attacker could exploit this vulnerability to cause a denial of service.

CVE-2022-28662 CVSS: 3.3

Siemens Simcenter Femap could allow a remote attacker to obtain sensitive information, caused by an out-of-bounds write when processing NEU files. By persuading a victim to open a specially-crafted NEU file, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system.

CVE-2022-28663 CVSS: 7.8

Siemens Simcenter Femap could allow a remote attacker to execute arbitrary code on the system, caused by an out-of-bounds write when processing NEU files. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system.

CVE-2022-28661 CVSS: 7.8

Siemens Simcenter Femap could allow a remote attacker to execute arbitrary code on the system, caused by an out-of-bounds read when processing NEU files. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system.

CVE-2022-25754 CVSS: 7.3

Siemens SCALANCE X-300 series is vulnerable to cross-site request forgery, caused by improper validation of user-supplied input. By persuading an authenticated user to visit a malicious Web site, a remote attacker could send a malformed HTTP request to carry out actions with the permissions of the victim. An attacker could exploit this vulnerability to perform cross-site scripting attacks, Web cache poisoning, and other malicious activities.

CVE-2022-25755 CVSS: 2.6

Siemens SCALANCE X-300 series could allow a remote attacker to obtain sensitive information, caused by missing security headers in the webserver. An attacker could exploit this vulnerability to obtain sensitive information and use this information to launch further attacks against the affected system.

CVE-2022-25756 CVSS: 7.9

Siemens SCALANCE X-300R series is vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute a script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

CVE-2022-26380 CVSS: 7.4

Siemens SCALANCE X-300 series is vulnerable to a denial of service, caused by an out-of-bounds read when a certain SNMP key exists. By sending a specially-crafted request, a remote attacker could exploit this vulnerability to cause the device to reboot.

Impact

- Denial of Service
- Information Disclosure
- Code Execution

Indicator Of Compromise

CVE

- CVE-2022-25622
- CVE-2022-25650
- CVE-2022-25751
- CVE-2022-25752

- CVE-2022-27194
- CVE-2022-27241
- CVE-2022-27480
- CVE-2022-27481
- CVE-2022-28328
- CVE-2022-28329
- CVE-2022-28662
- CVE-2022-28663
- CVE-2022-28661
- CVE-2022-25754
- CVE-2022-25755
- CVE-2022-25756
- CVE-2022-26380

Affected Vendors

Siemens

Affected Products

- Siemens SIMATIC S7-300
- Siemens Mendix Applications using Mendix 9
- Siemens SCALANCE X302-7 EEC
- Siemens SCALANCE X304-2FE
- Siemens SCALANCE X306-1LD FE
- Siemens TIA Portal 17
- Siemens SIMATIC PCS neo
- Siemens Mendix applications 9.10
- Siemens SICAM A8000 CP-8050
- Siemens SCALANCE W1788-1 M12
- Siemens SCALANCE W1788-2 EEC M12
- Siemens SCALANCE W1788-2IA M12
- Siemens Simcenter Femap 2022.1.1

Remediation

For patches, updates, and workarounds refer to the following vendor website:

Siemens