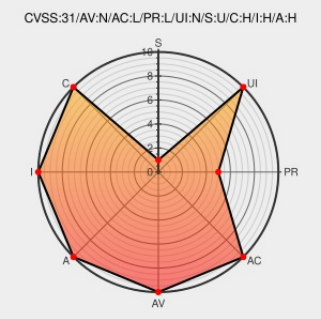
CVE-2022-2323

Published on: Not Yet Published

Last Modified on: 08/08/2022 04:12:00 PM UTC

CVE-2022-2323

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Sws12-10fpoe from Sonicwall contain the following vulnerability:

Improper neutralization of special elements used in a user input allows an authenticated malicious user to perform remote code execution in the host system. This vulnerability impacts SonicWall Switch 1.1.1.0-2s and earlier versions

CVE-2022-2323 has been assigned by PSIRT@sonicwall.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **SonicWall** - **SonicWall Switch** version **1.1.1.0-2s and earlier**

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Security Advisory	psirt.global.sonicwall.com text/html	CONFIRM psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0013

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Sonicwall	Sws12-10fpoe	-	All	All	All
Operating System	Sonicwall	Sws12-10fpoe Firmware	All	All	All	All
Hardware	Sonicwall	Sws12-8	-	All	All	All
Hardware	Sonicwall	Sws12-8poe	-	All	All	All
Operating System	Sonicwall	Sws12-8poe Firmware	All	All	All	All
Operating System	Sonicwall	Sws12-8 Firmware	All	All	All	All
Hardware	Sonicwall	Sws14-24	-	All	All	All
Hardware	Sonicwall	Sws14-24fpoe	-	All	All	All
Operating System	Sonicwall	Sws14-24fpoe Firmware	All	All	All	All
Operating System	Sonicwall	Sws14-24 Firmware	All	All	All	All
Hardware	Sonicwall	Sws14-48	-	All	All	All
Hardware	Sonicwall	Sws14-48fpoe	-	All	All	All
Operating System	Sonicwall	Sws14-48fpoe Firmware	All	All	All	All
Operating System	Sonicwall	Sws14-48 Firmware	All	All	All	All

cpe:2.3:h:sonicwall:sws12-10fpoe:-:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:sws12-10fpoe_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:sonicwall:sws12-8:-:*:*:*:*:*:*:*:

cpe:2.3:h:sonicwall:sws12-8poe:-:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:sws12-8poe_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:sws12-8_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:sonicwall:sws14-24:-:*:*:*:*:*:*:*:

cpe:2.3:h:sonicwall:sws14-24fpoe:-:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:sws14-24fpoe_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:sws14-24_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:sonicwall:sws14-48:-:*:*:*:*:*:*:*:

cpe:2.3:h:sonicwall:sws14-48fpoe:-:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:sws14-48fpoe_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:sonicwall:sws14-48_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@autumn_good_35	CVE-2022-2323 SonicWall Switch Post-Authenticated Remote Code Execution psirt.global.sonicwall.com/vuln-detail/SN…	2022-07-19 03:34:05
@CVEreport	CVE-2022-2323 : Improper neutralization of special elements used in a user input allows an authenticated malicious… twitter.com/i/web/status/1…	2022-07-29 19:18:21
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-2323 Improper neutralization of special elements used in a user input a… twitter.com/i/web/status/1…	2022-07-29 21:56:00
/r/netcve	CVE-2022-2323	2022-07-29 20:38:26

← Previous ID

Next ID→