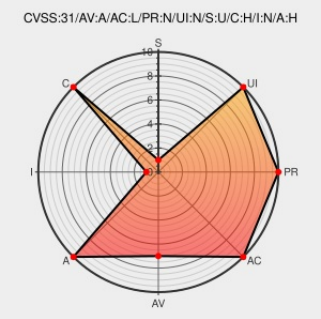
CVE-2021-20024

Published on: 07/09/2021 12:00:00 AM UTC

Last Modified on: 07/16/2021 04:59:00 PM UTC

CVE-2021-20024

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



Certain versions of Switch from Sonicwall contain the following vulnerability:

Multiple Out-of-Bound read vulnerability in SonicWall Switch when handling LLDP Protocol allows an attacker to cause a system instability or potentially read sensitive information from the memory locations.

CVE-2021-20024 has been assigned by PSIRT@sonicwall.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **SonicWall** - **SonicWall Switch** version **1.0.0.5-16 and earlier**

CVSS3 Score: 8.1 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	COMPLETE

CVE References

Description	Tags	Link
Security Advisory	psirt.global.sonicwall.com text/html	CONFIRM psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0011

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:o:sonicwall:switch:*:*:*:*:*:*:*:*:

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

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

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

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

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

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@autumn_good_35	CVE-2021-20024 SonicWall Switch LLDP Protocol multiple Out-of-Bound read vulnerability psirt.global.sonicwall.com/vuln-detail/SN…	2021-07-09 15:56:15
@CVEreport	CVE-2021-20024 : Multiple Out-of-Bound read vulnerability in SonicWall Switch when handling LLDP Protocol allows an… twitter.com/i/web/status/1…	2021-07-09 21:31:34
@threatmeter	CVE-2021-20024 Multiple Out-of-Bound read vulnerability in SonicWall Switch when handling	2021-07-10

	LLDP Protocol allows an a… twitter.com/i/web/status/1…	07:10:57
@threatmeter	SonicWALL Switch LLDP Protocol out-of-bounds read [CVE-2021-20024] A vulnerability was found in SonicWALL Switch (F… twitter.com/i/web/status/1…	2021-07-11 07:54:28
/r/netcve	CVE-2021-20024	2021-07-09 22:41:16

← Previous ID

Next ID→