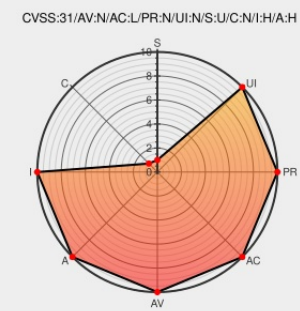
CVE-2022-4616

Published on: Not Yet Published

Last Modified on: 01/20/2023 07:56:00 AM UTC

CVE-2022-4616

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



Certain versions of Dx-3021I9 from Deltaww contain the following vulnerability:

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.

CVE-2022-4616 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Delta Industrial Automation** - **4G Router DX-3021** version **= 0**

CVSS3 Score: 9.1 - CRITICAL

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

CVE References

Description	Tags	Link
Delta 4G Router DX-3021 | CISA	www.cisa.gov text/html	MISC www.cisa.gov/uscert/ics/advisories/icsa-22-354-05
Delta | Download Center	downloadcenter.deltaww.com text/html	MISC downloadcenter.deltaww.com/en-US/DownloadCenter?v=1&CID=06&itemID=060308&downloadID=DX&dataType=12&sort_expr=cdate&sort_dir=DESC

Related QID Numbers

591318 Delta Industrial Automation 4G Router DX-3021 Command Injection Vulnerability (ICSA-22-354-05)

Exploit/POC from Github

This Python script aids in exploiting CVE-2022-46169 by automating payload delivery and response handling. It starts …

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Deltaww	Dx-3021l9	-	All	All	All
Operating System	Deltaww	Dx-3021l9 Firmware	All	All	All	All

cpe:2.3:h:deltaww:dx-3021l9:-:*:*:*:*:*:*:*:

cpe:2.3:o:deltaww:dx-3021l9_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/netcve	CVE-2022-4616	2023-01-13 01:38:58

← Previous ID

Next ID→