



CVE-2022-40691

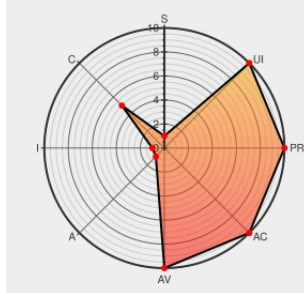
Published on: Not Yet Published

Last Modified on: 02/15/2023 06:49:00 PM UTC

CVE-2022-40691

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N



Certain versions of [Sds-3008](#) from [Moxa](#) contain the following vulnerability:

An information disclosure vulnerability exists in the web application functionality of Moxa SDS-3008 Series Industrial Ethernet Switch 2.1. A specially-crafted HTTP request can lead to a disclosure of sensitive information. An attacker can send an HTTP request to trigger this vulnerability.

CVE-2022-40691 has been assigned by [Cisco Talos](#) talos-cna@cisco.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Cisco](#) **Moxa** - **SDS-3008 Series Industrial Ethernet Switch** version = 2.1

CVSS3 Score: **5.3 - MEDIUM**

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

CVE References

Description	Tags	Link
TALOS-2022-1621 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	talosintelligence.com text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2022-1621
SDS-3008 Series Multiple Web Vulnerabilities	www.moxa.com text/html	MISC www.moxa.com/en/support/product-support/support/security-advisory/sds-3008-series-multiple-web-vulnerabilities

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.

Related QID Numbers

591353 Moxa SDS-3008 Series Multiple Vulnerabilities (MPSA-230101)

Exploit/POC from Github

An information disclosure vulnerability exists in the web application functionality of Moxa SDS-3008 Series Industria...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Moxa	Sds-3008	-	All	All	All
Hardware 	Moxa	Sds-3008-t	-	All	All	All
Operating System	Moxa	Sds-3008-t Firmware	All	All	All	All
Operating System	Moxa	Sds-3008 Firmware	All	All	All	All
cpe:2.3:h:moxa:sds-3008:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:moxa:sds-3008-t:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:moxa:sds-3008-t_firmware:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:moxa:sds-3008_firmware:~::~~::~~::~~::~~::~~::~~:::						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-40691 : An information disclosure vulnerability exists in the web application functionality of Moxa SDS-30... twitter.com/i/web/status/1...	2023-02-07 17:05:05
 /r/netcve	CVE-2022-40691	2023-02-07 17:39:51

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

