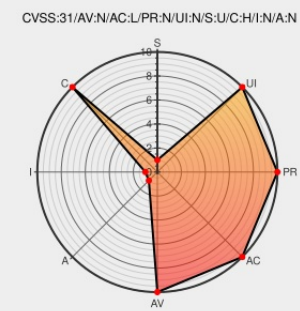
CVE-2021-45043

Published on: Not Yet Published

Last Modified on: 12/17/2021 05:09:00 PM UTC

CVE-2021-45043

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



Certain versions of Hd-network Real-time Monitoring System from Hd-network Real-time Monitoring System Project contain the following vulnerability:

HD-Network Real-time Monitoring System 2.0 allows ../ directory traversal to read /etc/shadow via the /language/lang s_Language parameter.

CVE-2021-45043 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
https://drive.google.com/file/d/1bx9yCN-IHYuRpd7g3jhMb0LcTC1ARzSX/view?usp=sharing	drive.google.com text/html Inactive Link Not Archived	MISC drive.google.com/file/d/1bx9yCN-IHYuRpd7g3jhMb0LcTC1ARzSX/view?usp=sharir
https://drive.google.com/file/d/1DlfZz0F8skWy3Mkahx_NMo-	drive.google.com	MISC

sYZh9-eun/view?usp=sharing text/html Inactive Link Not Archived drive.google.com/file/d/1DlfZz0F8skWy3Mkahx_N sYZh9-eun/view?usp=sharing

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

Exploit/POC from Github

HD-Network Real-time Monitoring System 2.0 allows ../ directory traversal to read /etc/shadow via the /language/lang …

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hd-network Real-time Monitoring System Project	Hd-network Real-time Monitoring System	2.0	All	All	All

cpe:2.3:a:hd-network_real-time_monitoring_system_project:hd-network_real-time_monitoring_system:2.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-45043 : HD-Network Real-time Monitoring System 2.0 allows ../ directory traversal to read /etc/shadow via… twitter.com/i/web/status/1…	2021-12-15 08:02:58
@hackplayers	My [CVE-2021–45043] LFI Write-up infosecwriteups.com/my-cve-2021-45…	2021-12-15 16:15:21
@threatmeter	CVE-2021-45043 HD-Network Real-time Monitoring System 2.0 allows ../ directory traversal to read /etc/shadow via th… twitter.com/i/web/status/1…	2021-12-15 23:08:52
@GobySec	?New vulnerability: HD-Network Real-time Monitoring System 2.0 Local File Inclusion (CVE-2021-45043) (RedTeam versi… twitter.com/i/web/status/1…	2021-12-16 08:46:35
/r/netcve	CVE-2021-45043	2021-12-15 09:38:11

← Previous ID Next ID→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report