

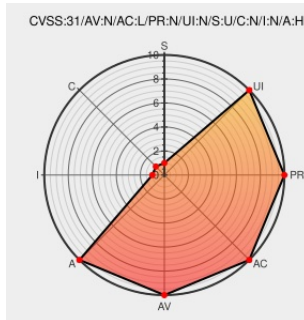


CVE-2022-3001

Published on: Not Yet Published

Last Modified on: 09/19/2022 07:08:00 PM UTC

CVE-2022-3001

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

Certain versions of [Video Management Systems](#) from [Milesight](#) contain the following vulnerability:

This vulnerability exists in Milesight Video Management Systems (VMS), all firmware versions prior to 40.7.0.79-r1, due to improper input handling at camera's web-based management interface. A remote attacker could exploit this vulnerability by sending a specially crafted http request on the targeted network camera. Successful exploitation of this vulnerability could allow the attacker to cause a Denial of Service condition on the targeted device.

CVE-2022-3001 has been assigned by [vdisclose@cert-in.org.in](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Milesight](#) - **Video Management Systems** version < 40.7.0.79-r1

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	NONE	NONE	HIGH

CVE References

Description	Tags	Link
No Description Provided	www.cert-in.org.in text/html	MISC www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2022-0352

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

This vulnerability exists in Milesight Video Management Systems (VMS), all firmware versions prior to 40.7.0.79-r1, d...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Milesight	Video Management Systems	-	All	All	All
Operating System	Milesight	Video Management Systems Firmware	All	All	All	All
Operating System	Milesight	Video Management Systems Firmware	40.7.0.79	-	All	All
cpe:2.3:h:milesight:video_management_systems:-:*:*:enterprise:*:*:						
cpe:2.3:o:milesight:video_management_systems_firmware:*:*:*:*:*:						
cpe:2.3:o:milesight:video_management_systems_firmware:40.7.0.79:-:*:*:*:*:						

Discovery Credit

This vulnerability is reported by Souvik Kandar and Arko Dhar from Redinent Innovations Engineering & Research Team, Karnataka, India

Social Mentions

Source	Title	Posted (UTC)
 /r/netcve	CVE-2022-3001	2022-09-15 15:39:06

[← 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)