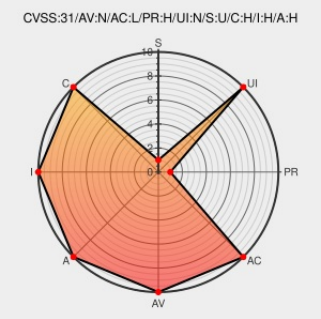
CVE-2023-25087

Published on: Not Yet Published

Last Modified on: 08/02/2023 03:29:00 PM UTC

CVE-2023-25087

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



Certain versions of Ur32l from Milesight contain the following vulnerability:

Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set function with the index and to_dport variables.

CVE-2023-25087 has been assigned by talos-cna@cisco.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Milesight** - **UR32L** version **= v32.3.0.5**

CVSS3 Score: 7.2 - HIGH

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

CVE References

Description	Tags	Link
TALOS-2023-1716 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	www.talosintelligence.com text/html	MISC www.talosintelligence.com/vulnerability_reports/TALOS-2023-1716
TALOS-2023-1716 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	talosintelligence.com text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2023-1716

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
Hardware	Milesight	Ur32l	-	All	All	All
Operating System	Milesight	Ur32l Firmware	32.3.0.5	All	All	All

cpe:2.3:h:milesight:ur32l:-:*:*:*:*:*:*:*:

cpe:2.3:o:milesight:ur32l_firmware:32.3.0.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-25087 : Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0… twitter.com/i/web/status/1…	2023-07-06 15:10:12

← Previous ID

Next ID→