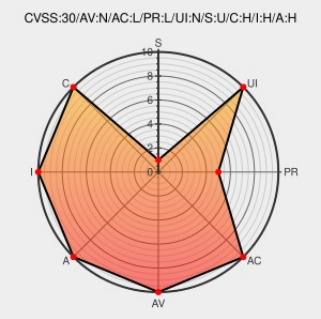
CVE-2017-12125

Published on: 05/14/2018 12:00:00 AM UTC

Last Modified on: 12/09/2022 01:51:00 AM UTC

CVE-2017-12125

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



Certain versions of Edr-810 from Moxa contain the following vulnerability:

An exploitable command injection vulnerability exists in the web server functionality of Moxa EDR-810 V4.1 build 17030317. A specially crafted HTTP POST can cause a privilege escalation resulting in root shell. An attacker can inject OS commands into the CN= parm in the "/goform/net_WebCSRGen" uri to trigger this vulnerability.

CVE-2017-12125 has been assigned by talos-cna@cisco.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Talos** - **Moxa** version **Moxa EDR-810 V4.1 build 17030317**

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
TALOS-2017-0477 || Cisco Talos Intelligence Group -	Exploit	MISC

Comprehensive Threat Intelligence	Third Party Advisory www.talosintelligence.com text/html	www.talosintelligence.com/vulnerability_reports/TALOS-2017-0477

Related QID Numbers

591014 Moxa EDR-810 Web Server Certificate Signing Request Command Injection Vulnerability (TALOS-2017-0477)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Moxa	Edr-810	-	All	All	All
Hardware	Moxa	Edr-810	-	All	All	All
Operating System	Moxa	Edr-810 Firmware	4.1	All	All	All
Operating System	Moxa	Edr-810 Firmware	4.1	All	All	All

cpe:2.3:h:moxa:edr-810:-:*:*:*:*:*:*:*:

cpe:2.3:h:moxa:edr-810:-:*:*:*:*:*:*:*:

cpe:2.3:o:moxa:edr-810_firmware:4.1:*:*:*:*:*:*:*:

cpe:2.3:o:moxa:edr-810_firmware:4.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→