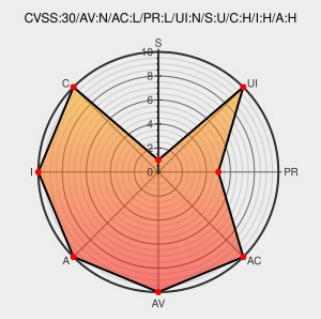
CVE-2020-8858

Published on: 02/13/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:59 PM UTC

CVE-2020-8858

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



Certain versions of Mgate 5105-mb-eip from Moxa contain the following vulnerability:

This vulnerability allows remote attackers to execute arbitrary code on affected installations of Moxa MGate 5105-MB-EIP firmware version 4.1. Authentication is required to exploit this vulnerability. The specific flaw exists within the DestIP parameter within MainPing.asp. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9552.

CVE-2020-8858 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Moxa** - **MGate 5105-MB-EIP** version **firmware version 4.1**

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
ZDI-20-214 | Zero Day Initiative	Third Party Advisory VDB Entry www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-20-214/
MGate 5105-MB-EIP Series Protocol Gateways Vulnerability	Vendor Advisory www.moxa.com text/html	MISC www.moxa.com/en/support/support/security-advisory/mgate-5105-mb-eip-series-protocol-gateways-vulnerability

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Moxa	Mgate 5105-mb-eip	-	All	All	All
Hardware	Moxa	Mgate 5105-mb-eip	-	All	All	All
Hardware	Moxa	Mgate 5105-mb-eip-t	-	All	All	All
Hardware	Moxa	Mgate 5105-mb-eip-t	-	All	All	All
Operating System	Moxa	Mgate 5105-mb-eip-t Firmware	All	All	All	All
Operating System	Moxa	Mgate 5105-mb-eip Firmware	All	All	All	All

cpe:2.3:h:moxa:mgate_5105-mb-eip:-:*:*:*:*:*:*:*:

cpe:2.3:h:moxa:mgate_5105-mb-eip:-:*:*:*:*:*:*:*:

cpe:2.3:h:moxa:mgate_5105-mb-eip-t:-:*:*:*:*:*:*:*:

cpe:2.3:h:moxa:mgate_5105-mb-eip-t:-:*:*:*:*:*:*:*:

cpe:2.3:o:moxa:mgate_5105-mb-eip-t_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:moxa:mgate_5105-mb-eip_firmware:*:*:*:*:*:*:*:*:

Discovery Credit

Dove Chiu, Philippe Lin, Charles Perine, Marco Balduzzi, Ryan Flores, Rainer Vosseler

← Previous ID

Next ID→

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