

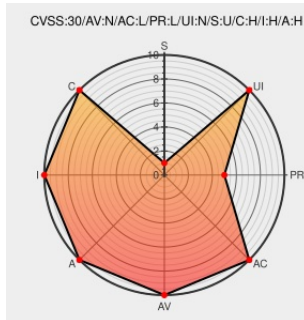


CVE-2020-8858

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

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

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 →](#)

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](#)