



CVE-2019-10963

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2019-10963
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-08 19:15:00 UTC
Updated	2021-10-28 13:24:00 UTC
Description	Moxa EDR 810, all versions 5.1 and prior, allows an unauthenticated attacker to be able to retrieve some log files from the c

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

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	All	All	All	All

References

Reference	Source	Link	Tags
Moxa EDR-810 Command Injection / Information Disclosure ≈ Packet Storm	MISC	packetstormsecurity.com	
Moxa EDR 810 Series CISA	MISC	www.us-cert.gov	Third Party Advisory, U
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[591309](#) Moxa EDR-810 Series Secure Routers Improper Input Validation Multiple Vulnerabilities (ICSA-19-274-03, MPESA-190906)

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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