



# CVE-2026-3868

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

## Summary

<b>CVE</b>	CVE-2026-3868
<b>State</b>	PUBLISHED
<b>Assigner</b>	Moxa
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-27 04:16:09 UTC
<b>Updated</b>	2026-04-27 04:16:09 UTC
<b>Description</b>	An improper handling of the length parameter inconsistency vulnerability has been identified in Moxa's Secure Router. Bec

## Risk And Classification

**Primary CVSS:** v4.0 8.7 HIGH from psirt@moxa.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**Problem Types:** CWE-130 | CWE-130 CWE-130: Improper Handling of Length Parameter Inconsistency

Version	Source	Type	Score	Severity	Vector
4.0	psirt@moxa.com	Secondary	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/C...
4.0	CNA	CVSS	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Moxa	EDR-8010 Series	affected 1.0 3.23 custom	Not specified
CNA	Moxa	EDR-8010 Series	unaffected 3.24 custom	Not specified
CNA	Moxa	EDR-G9010 Series	affected 1.0 3.23.1 custom	Not specified
CNA	Moxa	EDR-G9010 Series	unaffected 3.24 custom	Not specified

### References

Reference	Source	Link	Tags
www.moxa.com/en/support/product-support/security-advisory/mpsa-261521-cve-...	psirt@moxa.com	www.moxa.com	
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.

There are currently no legacy QID mappings associated with this CVE.

© 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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)