Cato's Socket WebUI is vulnerable to OS Command Injection

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-14213
State	PUBLISHED
Assigner	Cato
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-31 12:16:26 UTC
Updated	2026-04-01 14:24:02 UTC
Description	Cato Networks' Socket versions prior to 25 contain a command injection vulnerability that allows an authenticated attacker v

Risk And Classification

Primary CVSS: v4.0 8.3 HIGH from 2505284f-8ffb-486c-bf60-e19c1097a90b

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

EPSS: 0.004950000 probability, percentile 0.657360000 (date 2026-04-02)

Problem Types: CWE-20 | CWE-78 | CWE-78 CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | CWE-20 CWE-20 Improper Input Validation

Version	Source	Type	Score	Severity	Vector
4.0	2505284f-8ffb-486c-bf60-e19c1097a90b	Secondary	8.3	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:L/VA:H/
4.0	CNA	CVSS	8.3	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:L/VA:H/

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

High

Integrity

Low

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

High

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:L/VA:H/SC:N/SI:N/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/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	Cato Networks	Socket	affected 24 and below custom	Linux

References

Reference	Source
support.catonetworks.com/hc/en-us/articles/33184937283357-CVE-2025-14213-Socket-WebUI-...	2505284f-8ffb-486c-bf60-e19c1097a90b
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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