WatchGuard Firebox Insecure Deserialization in Fireware Access Portal

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-4266
State	PUBLISHED
Assigner	WatchGuard
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-30 13:16:22 UTC
Updated	2026-03-30 13:26:07 UTC
Description	An Insecure Deserialization vulnerability in WatchGuard Fireware OS allows an attacker that has obtained write access to t

Risk And Classification

Primary CVSS: v4.0 8.4 HIGH from 5d1c2695-1a31-4499-88ae-e847036fd7e3

CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000670000 probability, percentile 0.205930000 (date 2026-04-01)

Problem Types: CWE-502 | CWE-502 CWE-502 Deserialization of Untrusted Data

Version	Source	Type	Score	Severity	Vector
4.0	5d1c2695-1a31-4499-88ae-e847036fd7e3	Secondary	8.4	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:
4.0	CNA	CVSS	8.4	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/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/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	WatchGuard	Fireware OS	affected 12.1 12.11.8 semver	Not specified
CNA	WatchGuard	Fireware OS	affected 2025.1 2026.1.2 semver	Not specified

References

Reference	Source	Link	Tags
www.watchguard.com/wgrd-psirt/advisory/wgsa-2026-00007	5d1c2695-1a31-4499-88ae-e847036fd7e3	www.watchguard.com	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

Vendor Comments And Credit

Discovery Credit

CNA: btaol (en)

Additional Advisory Data

Exploits

CNA: WatchGuard is not aware of any exploitation of this issue in the wild.

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

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