GRID::Machine versions through 0.127 for Perl allows arbitrary code execution via unsafe deserialization

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-4851
State	PUBLISHED
Assigner	CPANSec
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-29 01:15:56 UTC
Updated	2026-04-01 15:23:23 UTC
Description	GRID::Machine versions through 0.127 for Perl allows arbitrary code execution via unsafe deserialization. GRID::Machine p

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.000670000 probability, percentile 0.206870000 (date 2026-04-01)

Problem Types: CWE-95 | CWE-502 | CWE-502 CWE-502 Deserialization of Untrusted Data | CWE-95 CWE-95 Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Casiano	Grid	\	machine	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	CASIANO	GRIDMachine	affected 0.127 custom	Not specified

References

Reference	Source	Link	Tags
www.openwall.com/lists/oss-security/2026/03/26/6	9b29abf9-4ab0-4765-b253-1875cd9b441e	www.openwall.com	Mailing List
www.openwall.com/lists/oss-security/2026/03/26/6	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	Mailing List
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Pied Crow crow@cpan.org (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-03-24T00:00:00.000Z	Vulnerability reported to module author and CPANSec
CNA	2026-03-25T00:00:00.000Z	CVE assigned by CPANSec
CNA	2026-03-26T00:00:00.000Z	Author confirmed module is unmaintained, no fix available
CNA	2026-03-26T00:00:00.000Z	Disclosed on oss-security mailing list

Workarounds

CNA: There is no fix available. If used, only connect to trusted remote hosts.

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

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