Amon2 versions before 6.17 for Perl use an insecure random_string implementation for security functions

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-15604
State	PUBLISHED
Assigner	CPANSec
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-28 19:16:53 UTC
Updated	2026-04-01 15:16:23 UTC
Description	Amon2 versions before 6.17 for Perl use an insecure random_string implementation for security functions. In versions 6.06

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: 0.000440000 probability, percentile 0.135570000 (date 2026-04-01)

Problem Types: CWE-338 | CWE-340 | CWE-340 CWE-340 Generation of Predictable Numbers or Identifiers | CWE-338 CWE-338 Use of Cryptographically Weak Pseudo-Random Number Generator

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	Tokuhirom	Amon2	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	TOKUHIROM	Amon2	affected 6.17 custom	Not specified

References

Reference	Source	Link
github.com/tokuhirom/Amon/pull/135	9b29abf9-4ab0-4765-b253-1875cd9b441e	github.com
www.openwall.com/lists/oss-security/2026/03/28/4	af854a3a-2127-422b-91ae-364da2661108	www.openwa
metacpan.org/release/TOKUHIROM/Amon2-6.17/changes	9b29abf9-4ab0-4765-b253-1875cd9b441e	metacpan.org
security.metacpan.org/docs/guides/random-data-for-security.html	9b29abf9-4ab0-4765-b253-1875cd9b441e	security.meta
metacpan.org/release/TOKUHIROM/Amon2-6.17/diff/TOKUHIROM/Amon2-6.16	9b29abf9-4ab0-4765-b253-1875cd9b441e	metacpan.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Solutions

CNA: Upgrade to Amon2 version 6.17 or later.

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