CVE-2026-34354

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-34354
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 16:16:10 UTC
Updated	2026-05-12 15:10:27 UTC
Description	Akamai Guardicore Platform Agent (GPA) and Zero Trust Client on Linux and macOS allow TOCTOU-based local privilege

Risk And Classification

Primary CVSS: v3.1 7.4 HIGH from cve@mitre.org

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

EPSS: 0.000110000 probability, percentile 0.012970000 (date 2026-05-12)

Problem Types: CWE-367 | CWE-367 CWE-367 Time-of-check Time-of-use (TOCTOU) Race Condition

Version	Source	Type	Score	Severity	Vector
3.1	cve@mitre.org	Secondary	7.4	HIGH	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.4	HIGH	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Akamai	Guardicore Platform Agent	affected 7.0 7.3.1 custom	Linux, macOS
CNA	Akamai	Zero Trust Client	affected 6.0 6.1.5 custom	Linux, macOS

References

Reference	Source	Link	Tags
www.akamai.com/blog/security-research/advisory-cve-2026-34354-guardicore-loc...	cve@mitre.org	www.akamai.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

No vendor comments have been submitted for this CVE.

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