



# CVE-2026-34354

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-34354
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-08 16:16:10 UTC
<b>Updated</b>	2026-05-12 15:10:27 UTC
<b>Description</b>	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

Integrity

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
<a href="http://www.akamai.com/blog/security-research/advisory-cve-2026-34354-guardicore-loc...">www.akamai.com/blog/security-research/advisory-cve-2026-34354-guardicore-loc...</a>	cve@mitre.org	<a href="http://www.akamai.com">www.akamai.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

Free CVE JSON API [cve.report/api](http://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](http://status.cve.report)