



# Chronosphere Chronocollector Information Disclosure Vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-0239
<b>State</b>	PUBLISHED
<b>Assigner</b>	palo_alto
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-13 19:16:57 UTC
<b>Updated</b>	2026-05-14 16:21:23 UTC
<b>Description</b>	An information disclosure vulnerability in the Chronosphere Chronocollector enables an unauthenticated attacker with network access to retrieve sensitive system information.

## Risk And Classification

**Primary CVSS:** v4.0 4.9 MEDIUM from psirt@paloaltonetworks.com

**CVSS:** 4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:N/R:U/V:C/RE:M/U:AMember

**EPSS:** 0.000210000 probability, percentile 0.060070000 (date 2026-05-17)

**Problem Types:** CWE-497 | CWE-497 CWE-497 Exposure of Sensitive System Information to an Unauthorized Control Sphere

Version	Source	Type	Score	Severity	Vector
4.0	psirt@paloaltonetworks.com	Secondary	4.9	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:N/R:U/V:C/RE:M/U:AMember
4.0	CNA	CVSS	4.9	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:N/R:U/V:C/RE:M/U:AMember

## CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:N/R:U/V:C/RE:M/U:A  
mber

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Palo Alto Networks</a>	<a href="#">Chronosphere Chronocollector</a>	affected 0.0.0 v0.116.0 custom	Not specified

#### References

Reference	Source	Link	Tags
<a href="https://security.paloaltonetworks.com/CVE-2026-0239">security.paloaltonetworks.com/CVE-2026-0239</a>	<a href="mailto:psirt@paloaltonetworks.com">psirt@paloaltonetworks.com</a>	<a href="https://security.paloaltonetworks.com">security.paloaltonetworks.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

#### Vendor Comments And Credit

Discovery Credit

**CNA:** Palo Alto Networks thanks our internal security research teams for discovering and reporting this issue. (en)

#### Additional Advisory Data

Source	Time	Event
CNA	2026-05-13T16:00:00.000Z	Initial publication.

Solutions

**CNA:** Version Suggested Solution Chronosphere Chronocollector Upgrade to v0.116.0 or later.

## Workarounds

**CNA:** No known workarounds exist for this issue.

## Exploits

**CNA:** Palo Alto Networks is not aware of any malicious exploitation of this issue.

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)