Chronosphere Chronocollector Information Disclosure Vulnerability

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

Summary

CVE	CVE-2026-0239
State	PUBLISHED
Assigner	palo_alto
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-13 19:16:57 UTC
Updated	2026-05-14 16:21:23 UTC
Description	An information disclosure vulnerability in the Chronosphere Chronocollector enables an unauthenticated attacker with netw

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/MSC:X/MSI:X/MSA:X/S:X/AU:N/R:U/V:C/RE:M/U:Amber

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/S
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/S

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/MSC:X/MSI:X/MSA:X/S:X/AU:N/R:U/V:C/RE:M/U:Amber

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Palo Alto Networks	Chronosphere Chronocollector	affected 0.0.0 v0.116.0 custom	Not specified

References

Reference	Source	Link	Tags
security.paloaltonetworks.com/CVE-2026-0239	psirt@paloaltonetworks.com	security.paloaltonetworks.com	
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: 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.