Coverity CLI Authentication Bypass

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-1496
State	PUBLISHED
Assigner	BlackDuck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-27 15:16:48 UTC
Updated	2026-03-30 13:26:29 UTC
Description	Vulnerable versions of Coverity Connect lack an error handler in the authentication logic for command line tooling that make

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from disclosure@synopsys.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:X/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:X/R:X/V:X/RE:X/U:X

EPSS: 0.000890000 probability, percentile 0.254050000 (date 2026-04-02)

Problem Types: CWE-639 | CWE-639 CWE-639 Authorization bypass through User-Controlled key

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@synopsys.com	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/S
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

ntegrity

High

vailability

None

ub Conf.

None

ub Integrity

None

ub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:X/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:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Black Duck	Coverity	affected 2024.3.0 2025.12.0 custom	Not specified
CNA	Black Duck	Coverity	unaffected 2024.3.0A	Not specified
CNA	Black Duck	Coverity	unaffected 2024.3.1A	Not specified
CNA	Black Duck	Coverity	unaffected 2024.3.2A	Not specified
CNA	Black Duck	Coverity	unaffected 2024.6.0A	Not specified
CNA	Black Duck	Coverity	unaffected 2024.6.1A	Not specified
CNA	Black Duck	Coverity	unaffected 2024.9.0A	Not specified
CNA	Black Duck	Coverity	unaffected 2024.9.1A	Not specified
CNA	Black Duck	Coverity	unaffected 2024.12.0A	Not specified
CNA	Black Duck	Coverity	unaffected 2024.12.1A	Not specified
CNA	Black Duck	Coverity	unaffected 2024.12.2	Not specified
CNA	Black Duck	Coverity	unaffected 2025.3.0A	Not specified
CNA	Black Duck	Coverity	unaffected 2025.3.1A	Not specified
CNA	Black Duck	Coverity	unaffected 2025.3.2	Not specified
CNA	Black Duck	Coverity	unaffected 2025.6.0A	Not specified
CNA	Black Duck	Coverity	unaffected 2025.6.2A	Not specified
CNA	Black Duck	Coverity	unaffected 2025.6.4	Not specified
CNA	Black Duck	Coverity	unaffected 2025.9.0A	Not specified
CNA	Black Duck	Coverity	unaffected 2025.9.2A	Not specified
CNA	Black Duck	Coverity	unaffected 2025.9.3	Not specified
CNA	Black Duck	Coverity	unaffected 2025.12.0A	Not specified

CNA	Black Duck	Coverity	unaffected 2025.12.1	Not specified

References

Reference	Source	Link
github.com/blackduck-inc/Coverity-Usage-Log-Analyzer	disclosure@synopsys.com	github.com
community.blackduck.com/s/article/Black-Duck-Security-Advisory-CVE-2026-1496	disclosure@synopsys.com	community.blackduc
community.blackduck.com/s/article/Instructions-on-how-to-block-token-endpoint-for-Cov...	disclosure@synopsys.com	community.blackduc
community.blackduck.com/s/article/WAF-IDS-IPS-Mitigation-Guidance	disclosure@synopsys.com	community.blackduc
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Huong Kieu from Cenobe (en)

Additional Advisory Data

Solutions

CNA: Customers are recommended to upgrade to one of the following Coverity patched versions at their earliest availability or deploy documented mitigations. Patched versions: * 2025.12.1 * 2025.12.0A * 2025.9.2A * 2025.9.0A * 2025.6.2A * 2025.6.0A * 2025.3.1A * 2025.3.0A * 2024.12.1A * 2024.12.0A * 2024.9.1A * 2024.9.0A Full Installers: * 2025.12.1 * 2025.9.3 * 2025.6.4 * 2025.3.2 * 2024.12.2

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