CVE-2025-6624

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

Summary

CVE	CVE-2025-6624
State	PUBLISHED
Assigner	snyk
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-06-26 05:15:23 UTC
Updated	2026-04-29 01:00:01 UTC
Description	Versions of the package snyk before 1.1297.3 are vulnerable to Insertion of Sensitive Information into Log File through loca

Risk And Classification

Primary CVSS: v4.0 1.2 LOW from report@snyk.io

CVSS:4.0/AV:L/AC:H/AT:P/PR:H/UI:P/VC:L/VI:N/VA:N/SC:H/SI:H/SA:H/E:P/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

Problem Types: CWE-532 | CWE-532 Insertion of Sensitive Information into Log File | CWE-532 CWE-532 Insertion of Sensitive Information into Log File

Version	Source	Type	Score	Severity	Vector
4.0	report@snyk.io	Secondary	1.2	LOW	CVSS:4.0/AV:L/AC:H/AT:P/PR:H/UI:P/VC:L/VI:N/VA:N/SC:H/SI:H/SA:H/E:P/C...
4.0	CNA	DECLARED	2.4	LOW	CVSS:4.0/AV:L/AC:H/AT:P/PR:H/UI:P/VC:L/VI:N/VA:N/SC:H/SI:H/SA:H/E:P
3.1	report@snyk.io	Secondary	7.2	HIGH	CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H
3.1	CNA	DECLARED	7.2	HIGH	CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H/E:P

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Attack Requirements

Present

Privileges Required

High

User Interaction

Passive

Confidentiality

Low

Integrity

None

Availability

None

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:L/AC:H/AT:P/PR:H/UI:P/VC:L/VI:N/VA:N/SC:H/SI:H/SA:H/E:P/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

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

High

User Interaction

Required

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Snyk	Snyk Cli	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	Snyk	affected 1.1297.3 semver	Not specified

References

Reference	Source	Link	Tags
github.com/snyk/go-application-framework/commit/ca7ba7d72e68455afb466a7a...	report@snyk.io	github.com	Patch
security.snyk.io/vuln/SNYK-JS-SNYK-10497607	report@snyk.io	security.snyk.io	Third Party Advisory
docs.snyk.io/snyk-cli/debugging-the-snyk-cli	report@snyk.io	docs.snyk.io	Technical Descriptior
github.com/snyk/cli/releases/tag/v1.1297.3	report@snyk.io	github.com	Release Notes
github.com/snyk/cli/commit/38322f377da7e5f1391e1f641710be50989fa4df	report@snyk.io	github.com	Patch
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: Snyk Research Team (en)

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