Improper Handling and Insufficient Isolation of Specific Temporary Files in Splunk Enterprise

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

Summary

CVE	CVE-2026-20204
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-15 16:16:34 UTC
Updated	2026-04-17 19:04:00 UTC
Description	In Splunk Enterprise versions below 10.2.1, 10.0.5, 9.4.10, and 9.3.11, and Splunk Cloud Platform versions below 10.4.260

Risk And Classification

Primary CVSS: v3.1 7.1 HIGH from psirt@cisco.com

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

EPSS: 0.001310000 probability, percentile 0.325800000 (date 2026-04-20)

Problem Types: CWE-377 | CWE-377 Creating and using insecure temporary files can leave application and system data vulnerable to attack.

Version	Source	Type	Score	Severity	Vector
3.1	psirt@cisco.com	Primary	7.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

Required

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Splunk	Splunk	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Splunk	Splunk Enterprise	affected 10.2 10.2.1 custom	Not specified
CNA	Splunk	Splunk Enterprise	affected 10.0 10.0.5 custom	Not specified
CNA	Splunk	Splunk Enterprise	affected 9.4 9.4.10 custom	Not specified
CNA	Splunk	Splunk Enterprise	affected 9.3 9.3.11 custom	Not specified
CNA	Splunk	Splunk Cloud Platform	affected 10.4.2603 Not Affected custom	Not specified
CNA	Splunk	Splunk Cloud Platform	affected 10.3.2512 10.3.2512.5 custom	Not specified
CNA	Splunk	Splunk Cloud Platform	affected 10.2.2510 10.2.2510.9 custom	Not specified
CNA	Splunk	Splunk Cloud Platform	affected 10.1.2507 10.1.2507.19 custom	Not specified
CNA	Splunk	Splunk Cloud Platform	affected 10.0.2503 10.0.2503.13 custom	Not specified
CNA	Splunk	Splunk Cloud Platform	affected 9.3.2411 9.3.2411.127 custom	Not specified

References

Reference	Source	Link	Tags
advisory.splunk.com/advisories/SVD-2026-0403	psirt@cisco.com	advisory.splunk.com	Vendor Advisory
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: Gabriel Nitu, Splunk (en)

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report