Cisco Nexus Dashboard Insights Arbitrary File Write Vulnerability

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-20174
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-01 17:28:31 UTC
Updated	2026-04-01 17:28:31 UTC
Description	A vulnerability in the Metadata update feature of Cisco Nexus Dashboard Insights could allow an authenticated, remote atta

Risk And Classification

Primary CVSS: v3.1 4.9 MEDIUM from psirt@cisco.com

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

Problem Types: CWE-22 | CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
3.1	psirt@cisco.com	Primary	4.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N
3.1	CNA	CVSSV3_1	4.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Integrity

High

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Cisco	Cisco Nexus Dashboard	affected 3.1(1k)	Not specified
CNA	Cisco	Cisco Nexus Dashboard	affected 3.1(1l)	Not specified
CNA	Cisco	Cisco Nexus Dashboard	affected 3.2(1e)	Not specified
CNA	Cisco	Cisco Nexus Dashboard	affected 3.2(1i)	Not specified
CNA	Cisco	Cisco Nexus Dashboard	affected 3.3(1a)	Not specified
CNA	Cisco	Cisco Nexus Dashboard	affected 3.3(1b)	Not specified
CNA	Cisco	Cisco Nexus Dashboard	affected 3.3(2b)	Not specified
CNA	Cisco	Cisco Nexus Dashboard	affected 4.0(1i)	Not specified
CNA	Cisco	Cisco Nexus Dashboard	affected 3.3(2g)	Not specified
CNA	Cisco	Cisco Nexus Dashboard	affected 3.2(2f)	Not specified
CNA	Cisco	Cisco Nexus Dashboard	affected 3.2(2g)	Not specified
CNA	Cisco	Cisco Nexus Dashboard	affected 3.2(2m)	Not specified
CNA	Cisco	Cisco Nexus Dashboard	affected 3.1(1n)	Not specified
CNA	Cisco	Cisco Nexus Dashboard	affected 4.1(1g)	Not specified
CNA	Cisco	Cisco Nexus Dashboard Insights	affected 2.2.2.125	Not specified
CNA	Cisco	Cisco Nexus Dashboard Insights	affected 2.2.2.126	Not specified
CNA	Cisco	Cisco Nexus Dashboard Insights	affected 5.0.1.150	Not specified
CNA	Cisco	Cisco Nexus Dashboard Insights	affected 5.0.1.154	Not specified
CNA	Cisco	Cisco Nexus Dashboard Insights	affected 5.1.0.131	Not specified
CNA	Cisco	Cisco Nexus Dashboard Insights	affected 5.1.0.135	Not specified
CNA	Cisco	Cisco Nexus Dashboard Insights	affected 6.0.1	Not specified
CNA	Cisco	Cisco Nexus Dashboard Insights	affected 6.0.2	Not specified
CNA	Cisco	Cisco Nexus Dashboard Insights	affected 6.1.1	Not specified
CNA	Cisco	Cisco Nexus Dashboard Insights	affected 6.1.2	Not specified
CNA	Cisco	Cisco Nexus Dashboard Insights	affected 6.1.3	Not specified
CNA	Cisco	Cisco Nexus Dashboard Insights	affected 6.2.1	Not specified
CNA	Cisco	Cisco Nexus Dashboard Insights	affected 6.2.2	Not specified
CNA	Cisco	Cisco Nexus Dashboard Insights	affected 6.3.1	Not specified

CNA	Cisco	Cisco Nexus Dashboard Insights	affected 6.4.1	Not specified

References

Reference	Source	Link	Tag
sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndi-af...	psirt@cisco.com	sec.cloudapps.cisco.com	
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Exploits

CNA: The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

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 registred 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.

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