



Nomad vulnerable to arbitrary file read/write on client host through symlink attack

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-6959
State	PUBLISHED
Assigner	HashiCorp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-12 20:16:46 UTC
Updated	2026-05-12 20:16:46 UTC
Description	HashiCorp Nomad and Nomad Enterprise prior to 2.0.1 are vulnerable to arbitrary file read and write on the client host as tr

Risk And Classification

Primary CVSS: v3.1 6 MEDIUM from security@hashicorp.com

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

Problem Types: CWE-59 | CWE-59 CWE-59: Improper Link Resolution Before File Access (Link Following)

Version	Source	Type	Score	Severity	Vector
3.1	security@hashicorp.com	Secondary	6	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:N
3.1	CNA	CVSS	6	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Changed

Confidentiality

None

Integrity

None

High

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	HashiCorp	Nomad	affected 0.9.0 2.0.1 semver	64 bit, 32 bit, x86, ARM, MacOS, Windows, Linux
CNA	HashiCorp	Nomad Enterprise	affected 0.9.0 2.0.1 semver	64 bit, 32 bit, x86, ARM, MacOS, Windows, Linux

References

Reference	Source	Link
discuss.hashicorp.com/t/hcsec-2026-14-nomad-arbitrary-file-read-write-on-client-hos...	security@hashicorp.com	discuss.hashicorp.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: This issue was identified by Alex Manson (Aiven / NeuroWinter). (en)

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 registered 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](#).

Free CVE JSON API cve.report/api

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