



# Consul-template vulnerable to sandbox path bypass in file helper via a symlink attack

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

## Summary

<b>CVE</b>	CVE-2026-5061
<b>State</b>	PUBLISHED
<b>Assigner</b>	HashiCorp
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-12 15:16:16 UTC
<b>Updated</b>	2026-05-12 15:16:16 UTC
<b>Description</b>	The consul-template library before version 0.42.0 is vulnerable to a sandbox path bypass in the file template helper that ma

## Risk And Classification

**Primary CVSS:** v3.1 4.7 MEDIUM from security@hashicorp.com

**CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/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	4.7	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	CVSS	4.7	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	HashiCorp	Tooling	affected 0.1.0 0.42.0 semver	64 bit, 32 bit, x86, ARM, MacOS, Windows, Linux

### References

Reference	Source	Link
discuss.hashicorp.com/t/hcsec-2026-12-consul-template-vulnerable-to-sandbox-path-by...	security@hashicorp.com	<a href="https://discuss.hashicorp.com/t/hcsec-2026-12-consul-template-vulnerable-to-sandbox-path-by-...">discuss.hashicorp.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

### Vendor Comments And Credit

#### Discovery Credit

**CNA:** This issue was reported to HashiCorp by Mohamed Abdelaal (0xmrma). (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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)