



# OpenHands is Vulnerable to Command Injection through its Git Diff Handler

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

## Summary

<b>CVE</b>	CVE-2026-33718
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-27 01:16:19 UTC
<b>Updated</b>	2026-03-30 13:26:29 UTC
<b>Description</b>	OpenHands is software for AI-driven development. Starting in version 1.5.0, a Command Injection vulnerability exists in the

## Risk And Classification

**Primary CVSS:** v3.1 7.6 HIGH from security-advisories@github.com

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

**EPSS:** 0.002270000 probability, percentile 0.453980000 (date 2026-04-01)

**Problem Types:** CWE-78 | CWE-78 CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	7.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L
3.1	CNA	DECLARED	7.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

Low

Availability

Low

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	OpenHands	OpenHands	affected < 1.5.0	Not specified

### References

Reference	Source	Link	Tags
github.com/OpenHands/OpenHands/pull/13051	security-advisories@github.com	github.com	
docs.python.org/3/library/shlex.html	security-advisories@github.com	docs.python.org	
docs.python.org/3/library/subprocess.html	security-advisories@github.com	docs.python.org	
owasp.org/www-community/attacks/Command_Injection	security-advisories@github.com	owasp.org	
github.com/OpenHands/OpenHands/security/advisories/GHSA-7h8w-hj9j-8rjw	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

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.

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