



# OpenHarness SSRF via web\_fetch and web\_search

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

## Summary

<b>CVE</b>	CVE-2026-40516
<b>State</b>	PUBLISHED
<b>Assigner</b>	VulnCheck
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-17 17:17:09 UTC
<b>Updated</b>	2026-04-17 19:01:56 UTC
<b>Description</b>	OpenHarness before commit bd4df81 contains a server-side request forgery vulnerability in the web_fetch and web_search

## Risk And Classification

**Primary CVSS:** v4.0 7.8 HIGH from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:H/SI:L/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000360000 probability, percentile 0.104280000 (date 2026-04-18)

**Problem Types:** CWE-918 | CWE-918 CWE-918 Server-Side Request Forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	7.8	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:H/SI:L/SA
4.0	CNA	CVSS	7.8	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:H/SI:L/SA
3.1	disclosure@vulncheck.com	Primary	8.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L
3.1	CNA	CVSS	8.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

None

Confidentiality

None

Integrity

Low

Availability

None

Sub Conf.

High

Sub Integrity

Low

Sub Availability

Low

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:H/SI:L/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

Low

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	HKUDS	OpenHarness	affected bd4df81f634f8c7cddcc3fdf7f561a13dcbf03ae git	Not specified

### References

Reference	Source	Link
github.com/HKUDS/OpenHarness/commit/bd4df81f634f8c7cddcc3fdf7f561a13dcbf03ae	disclosure@windtalk.com	github.com

github.com/HKUDS/OpenHarness/commit/ba4a1817b34f8c7caacc31a175b1a13acbd...	disclosure@vulncheck.com	github.com
www.vulncheck.com/advisories/openharness-ssrf-via-web-fetch-and-web-search	disclosure@vulncheck.com	www.vulncheck.com
github.com/HKUDS/OpenHarness/pull/92	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

## Vendor Comments And Credit

### Discovery Credit

**CNA:** Chia Min Jun Lennon (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](#)