



# OpenHarness Improper Access Control via File Tools

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-22682
<b>State</b>	PUBLISHED
<b>Assigner</b>	VulnCheck
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-07 18:16:39 UTC
<b>Updated</b>	2026-04-16 16:15:56 UTC
<b>Description</b>	OpenHarness prior to commit 166fcfe contains an improper access control vulnerability in built-in file tools due to inconsiste

## Risk And Classification

**Primary CVSS:** v4.0 8.4 HIGH from disclosure@vulncheck.com

**CVSS:**4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/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:** 0.000100000 probability, percentile 0.010720000 (date 2026-04-13)

**Problem Types:** CWE-863 | CWE-863 CWE-863 Incorrect Authorization

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	8.4	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA
4.0	CNA	CVSS	8.4	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA
3.1	disclosure@vulncheck.com	Primary	7.1	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
3.1	CNA	CVSS	7.1	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

## CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

None

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/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

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	HKUDS	OpenHarness	affected 166fcfefb7614dbac51bd061f56542725b0298e9 git	Not specified

### References

Reference	Source	Link
www.wydsback.com/advisories/openharness-impersonation-escape-control-via-file-tools	disclosure@wydsback.com	www.wydsback.com

<a href="http://www.vuincneck.com/advisories/openharness-improper-access-control-via-r11e-tools">www.vuincneck.com/advisories/openharness-improper-access-control-via-r11e-tools</a>	<a href="mailto:disclosure@vuincneck.com">disclosure@vuincneck.com</a>	<a href="http://www.vuincneck.com">www.vuincneck.com</a>
<a href="https://github.com/HKUDS/OpenHarness/commit/166fcfefb7614dbac51bd061f56542725b02...">github.com/HKUDS/OpenHarness/commit/166fcfefb7614dbac51bd061f56542725b02...</a>	<a href="mailto:disclosure@vulncheck.com">disclosure@vulncheck.com</a>	<a href="https://github.com">github.com</a>
<a href="https://github.com/HKUDS/OpenHarness/pull/32">github.com/HKUDS/OpenHarness/pull/32</a>	<a href="mailto:disclosure@vulncheck.com">disclosure@vulncheck.com</a>	<a href="https://github.com">github.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

## 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](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

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)