



# Zoraxy: Authenticated Path Traversal in Config Import leads to RCE

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

## Summary

<b>CVE</b>	CVE-2026-33529
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-26 20:16:15 UTC
<b>Updated</b>	2026-04-02 18:13:03 UTC
<b>Description</b>	Zoraxy is a general purpose HTTP reverse proxy and forwarding tool. Prior to version 3.3.2, an authenticated path traversal

## Risk And Classification

**Primary CVSS:** v3.1 8.8 HIGH from nvd@nist.gov

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

**EPSS:** 0.000530000 probability, percentile 0.167020000 (date 2026-04-01)

**Problem Types:** CWE-22 | CWE-22 CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	security-advisories@github.com	Secondary	3.3	LOW	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:N
3.1	CNA	DECLARED	3.3	LOW	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

#### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zoraxy	Zoraxy	All	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Tobychui	Zoraxy	affected < 3.3.2	Not specified

#### References

Reference	Source	Link	Tag
github.com/tobychui/zoraxy/releases/tag/v3.3.2	security-advisories@github.com	github.com	Release
github.com/tobychui/zoraxy/security/advisories/GHSA-7pq3-326h-f8q9	security-advisories@github.com	github.com	Exploit
github.com/tobychui/zoraxy/commit/69ac755aeec5d15ba4c62099f7f1ed77a855b40b	security-advisories@github.com	github.com	Patch
CVE Program record	CVE.ORG	www.cve.org	Canonical
NVD vulnerability detail	NVD	nvd.nist.gov	Canonical

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](#)**