



# XenForo Open Redirect via getDynamicRedirect

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

## Summary

<b>CVE</b>	CVE-2024-58342
<b>State</b>	PUBLISHED
<b>Assigner</b>	VulnCheck
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-01 01:16:39 UTC
<b>Updated</b>	2026-04-01 18:54:10 UTC
<b>Description</b>	XenForo before 2.2.17 and 2.3.1 allows open redirect via a specially crafted URL. The getDynamicRedirect() function does

## Risk And Classification

**Primary CVSS:** v4.0 5.3 MEDIUM from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:L/VA:L/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:** 0.000310000 probability, percentile 0.086960000 (date 2026-04-01)

**Problem Types:** CWE-601 | CWE-601 URL Redirection to Untrusted Site ('Open Redirect')

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:L/VA:L/SC:N/SI:N/SA
4.0	CNA	CVSS	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:L/VA:L/SC:N/SI:N/SA
3.1	nvd@nist.gov	Primary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	disclosure@vulncheck.com	Secondary	6.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L
3.1	CNA	CVSS	6.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Passive

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:L/VA:L/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/MS:C:X/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

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xenforo	Xenforo	All	All	All	All
Application	Xenforo	Xenforo	2.3.0	All	All	All

### Vendor Declared Affected Products

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	XenForo	XenForo	affected 2.2.17 semver	Not specified
CNA	XenForo	XenForo	affected 2.3.0 2.3.1 semver	Not specified

References

Reference	Source	Link	Tags
xenforo.com/community/threads/xenforo-2-2-17-released-security-fix.227797	disclosure@vulncheck.com	<a href="https://xenforo.com">xenforo.com</a>	Release
www.vulncheck.com/advisories/xenforo-open-redirect-via-getdynamicredirect	disclosure@vulncheck.com	<a href="https://www.vulncheck.com">www.vulncheck.com</a>	Third Pa
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonica
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonica

Vendor Comments And Credit

Discovery Credit

**CNA:** mattrogowski (en)

**CNA:** Jake B. (en)

**CNA:** ThemeHouse (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](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/licenses).

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