



# wpForo Forum <= 2.1.7 - Authenticated (Subscriber+) Local File Include, Server-Side Request Forgery, and PHAR Deserialization via file\_get\_contents

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

## Summary

<b>CVE</b>	CVE-2023-2249
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-06-09 06:16:05 UTC
<b>Updated</b>	2026-04-08 18:17:58 UTC
<b>Description</b>	The wpForo Forum plugin for WordPress is vulnerable to Local File Include, Server-Side Request Forgery, and PHAR Deserialization via file_get_contents.

## 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

**Problem Types:** CWE-98 | CWE-829 | CWE-918 | CWE-98 CWE-98 Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')

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@wordfence.com	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

## 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	Gvectors	Wpforo Forum	All	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Tomdever	WpForo Forum	affected 2.1.7 semver	Not specified

#### References

##### Reference

403 Forbidden

403 Forbidden

wpForo Forum <= 2.1.7 - Authenticated (Subscriber+) Local File Include, Server-Side Request Forgery, and PHAR Deserialization via file\_get

CVE Program record

NVD vulnerability detail

#### Vendor Comments And Credit

Discovery Credit

**CNA:** Hamed (en)

#### Additional Advisory Data

Source	Time	Event
CNA	2023-04-24T00:00:00.000Z	Vendor Notified
CNA	2023-06-01T00:00:00.000Z	Disclosed

There are currently no legacy QID mappings associated with this CVE.

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](#)