



# Froxlор has Local File Inclusion via path traversal in API `def\_language` parameter that leads to Remote Code Execution

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2026-41228   |
| <b>State</b>           | PUBLISHED  |
| <b>Assigner</b>        | GitHub_M   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2026-04-23 04:16:19 UTC  |
| <b>Updated</b>         | 2026-04-23 04:16:19 UTC  |
| <b>Description</b>     | Froxlор is open source server administration software. Prior to version 2.3.6, the Froxlор API endpoint `Customers.update` ( |

## Risk And Classification

**Primary CVSS:** v3.1 9.9 CRITICAL from security-advisories@github.com

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

**Problem Types:** CWE-98 | 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     | security-advisories@github.com | Secondary | 9.9   | CRITICAL | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H |
| 3.1     | CNA                            | DECLARED  | 10    | CRITICAL | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

### Vendor Declared Affected Products

| Source | Vendor  | Product | Version          | Platforms     |
|--------|---------|---------|------------------|---------------|
| CNA    | Froxlор | Froxlор | affected < 2.3.6 | Not specified |

### References

| Reference  | Source                         | Link         | Tags      |
|--|--------------------------------|--------------|-----------|
| github.com/froxlор/froxlор/releases/tag/2.3.6                              | security-advisories@github.com | github.com   |           |
| github.com/froxlор/froxlор/commit/bc5e6dbaa90e6f3573129da640595e8c770e1d0c | security-advisories@github.com | github.com   |           |
| github.com/froxlор/froxlор/security/advisories/GHSA-w59f-67xm-rxx7         | security-advisories@github.com | github.com   |           |
| 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.

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)