



Redirect-based SSRF leading to internal network access in curl_cffi (with TLS impersonation bypass)

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2026-33752 |
| State | PUBLISHED |
| Assigner | GitHub_M |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-04-06 16:16:34 UTC |
| Updated | 2026-04-09 18:10:21 UTC |
| Description | curl_cffi is the a Python binding for curl. Prior to 0.15.0, curl_cffi does not restrict requests to internal IP ranges, and follows |

Risk And Classification

Primary CVSS: v3.1 8.6 HIGH from security-advisories@github.com

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

EPSS: 0.000100000 probability, percentile 0.011770000 (date 2026-04-07)

Problem Types: CWE-918 | CWE-918 CWE-918: Server-Side Request Forgery (SSRF)

| Version | Source | Type | Score | Severity | Vector |
|---------|--------------------------------|-----------|-------|----------|--|
| 3.1 | security-advisories@github.com | Secondary | 8.6 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N |
| 3.1 | CNA | DECLARED | 8.6 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N |

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|----------------------------|---------------------------|---------|--------|---------|----------|
| Application | Lexiforest | Curl Cffi | All | All | All | All |
| Application | Lexiforest | Curl Cffi | 0.15.0 | beta1 | All | All |
| Application | Lexiforest | Curl Cffi | 0.15.0 | beta2 | All | All |
| Application | Lexiforest | Curl Cffi | 0.15.0 | beta3 | All | All |
| Application | Lexiforest | Curl Cffi | 0.15.0 | beta4 | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|----------------------------|---------------------------|-------------------|---------------|
| CNA | Lexiforest | Curl Cffi | affected < 0.15.0 | Not specified |

References

| Reference | Source | Link | Tags |
|---|--------------------------------------|---|-----------|
| github.com/lexiforest/curl_cffi/security/advisories/GHSA-qw2m-4pqf-rmpp | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | github.com | Exploit |
| 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

CVE.report and Source URL Uptime Status status.cve.report