



WordPress Envato Elements plugin <= 2.0.14 - Server Side Request Forgery (SSRF) vulnerability

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

Summary

CVE CVE-2024-56275

State PUBLISHED

Assigner Patchstack

Source Priority CVE Program / NVD first with legacy fallback

Published 2025-01-07 11:15:09 UTC

Updated 2026-04-28 19:28:07 UTC

Description Server-Side Request Forgery (SSRF) vulnerability in Envato Envato Elements allows Server Side Request Forgery. This iss

Risk And Classification

Primary CVSS: v3.1 4.1 MEDIUM from audit@patchstack.com

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

EPSS: 0.001330000 probability, percentile 0.324900000 (date 2026-04-28)

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

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	4.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N
3.1	CNA	CVSS	4.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Changed

Confidentiality

Low

Integrity

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Envato	Envato Elements	affected n/a 2.0.14 custom	Not specified

References

Reference

[patchstack.com/database/wordpress/plugin/envato-elements/vulnerability/wordp...](https://patchstack.com/database/wordpress/plugin/envato-elements/vulnerability/wordpress-envato-elements-plugin-2-0-14-server-side-request-forgery)

<https://patchstack.com/database/wordpress/plugin/envato-elements/vulnerability/wordpress-envato-elements-plugin-2-0-14-server-side-request-forgery>

[CVE Program record](#)

[NVD vulnerability detail](#)

Vendor Comments And Credit

Discovery Credit

CNA: [Rafie Muhammad \(Patchstack\)](#) (en)

Additional Advisory Data

Solutions

CNA: Update the WordPress Envato Elements plugin to the latest available version (at least 2.0.15).

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](#)