



Unlimited Elements For Elementor (Free Widgets, Addons, Templates) <= 1.5.102 - Authenticated (Admin+) Command Injection

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

Summary

CVE	CVE-2024-2662
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-05-14 15:20:17 UTC
Updated	2026-04-08 18:21:10 UTC
Description	The Unlimited Elements For Elementor (Free Widgets, Addons, Templates) plugin for WordPress is vulnerable to command injection in the <code>unlimited_elements.php</code> file. An authenticated user with the <code>administrator</code> role can trigger a command injection via the <code>wp_ajax_unlimited_elements_load_widgets</code> endpoint. The attacker can execute arbitrary OS commands with the privileges of the user running the plugin. This vulnerability affects versions of the plugin up to and including 1.5.102.

Risk And Classification

Primary CVSS: v3.1 7.2 HIGH from security@wordfence.com

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

Problem Types: CWE-78 | CWE-78 CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:H/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	Unlimited-elements	Unlimited Elements For Elementor	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Unitecms	Unlimited Elements For Elementor	affected 1.5.102 semver	Not specified

References

Reference	Source
plugins.trac.wordpress.org/changeset/3071404/unlimited-elements-for-elementor/trunk/inc_...	af854a3a-2127-422b-91ae-364da2661108
www.wordfence.com/threat-intel/vulnerabilities/id/58492dbb-b9e0-4477-b85d-ace06...	af854a3a-2127-422b-91ae-364da2661108
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: wesley (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-05-09T19:02:36.000Z	Disclosed

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