Xelion Webchat <= 9.1.0 - Authenticated (Subscriber+) Arbitrary Options Update

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-3058
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-04-24 09:15:30 UTC
Updated	2026-04-08 17:20:39 UTC
Description	The Xelion Webchat plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escal

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from security@wordfence.com

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

Problem Types: CWE-862 | CWE-862 CWE-862 Missing Authorization

Version	Source	Type	Score	Severity	Vector
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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Jauharixelion	Xelion Webchat	affected 9.1.0 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/changeset	security@wordfence.com	plugins.trac.wordpr
plugins.trac.wordpress.org/browser/xelion-webchat/trunk//includes/class-xelion-webchat-a...	security@wordfence.com	plugins.trac.wordpr
www.wordfence.com/threat-intel/vulnerabilities/id/250202d5-3a0d-494c-8386-1f4cd...	security@wordfence.com	www.wordfence.cor
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Kenneth Dunn (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-04-23T19:47:14.000Z	Disclosed

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