Flynax Bridge <= 2.2.0 - Unauthenticated Privilege Escalation via Password Update

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

Summary

CVE	CVE-2025-3603
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-04-24 09:15:31 UTC
Updated	2026-04-08 19:24:03 UTC
Description	The Flynax Bridge plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from security@wordfence.com

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

EPSS: 0.007300000 probability, percentile 0.726590000 (date 2026-04-13)

Problem Types: CWE-620 | CWE-620 CWE-620 Unverified Password Change

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/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	Flynax	Flynax Bridge	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	V1rustyle	Flynax Bridge	affected 2.2.0 semver	Not specified

References

Reference	Source	Link
www.wordfence.com/threat-intel/vulnerabilities/id/fa8124db-ee6a-481d-88c6-4cc84...	security@wordfence.com	www.wordfence.com
plugins.trac.wordpress.org/changeset/3306501	security@wordfence.com	plugins.trac.wordpress.org
plugins.trac.wordpress.org/browser/flynax-bridge/trunk/request.php	security@wordfence.com	plugins.trac.wordpress.org
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	2025-04-23T19:43:49.000Z	Disclosed

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

Free CVE JSON API cve.report/api

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