



WP STAGING <= 3.4.3 and WP STAGING Pro <= 5.4.3 - Sensitive Information Exposure via Log File

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2024-3682
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-04-26 10:15:11 UTC
Updated	2026-04-08 18:21:31 UTC
Description	The WP STAGING and WP STAGING Pro plugins for WordPress are vulnerable to Sensitive Information Exposure in versi

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from security@wordfence.com

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

Problem Types: CWE-200 | CWE-200 CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	DECLARED	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown	
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Renehermi	WP STAGING WordPress Backup Restore Migration	affected 3.4.3 semver	Not specified
CNA	WPStaging	WP STAGING Pro WordPress Backup Plugin	affected 5.4.3 semver	Not specified

References

Reference	Source	Link
wp-staging.com/wp-staging-pro-changelog	af854a3a-2127-422b-91ae-364da2661108	wp-stag
www.wordfence.com/threat-intel/vulnerabilities/id/75eab54b-dbe0-4440-b4ab-601c5...	af854a3a-2127-422b-91ae-364da2661108	www.wc
wp-staging.com/wp-staging-changelog	af854a3a-2127-422b-91ae-364da2661108	wp-stag
plugins.trac.wordpress.org/changeset/3076275/wp-staging	af854a3a-2127-422b-91ae-364da2661108	plugins.
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

Vendor Comments And Credit

Discovery Credit

CNA: haidv35 (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-04-15T00:00:00.000Z	Vendor Notified
CNA	2024-04-25T00:00:00.000Z	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