



# Backup Bolt <= 1.4.1 - Authenticated (Admin+) Arbitrary File Download

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

## Summary

<b>CVE</b>	CVE-2025-10306
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-10-03 12:15:42 UTC
<b>Updated</b>	2026-04-08 18:23:11 UTC
<b>Description</b>	The Backup Bolt plugin for WordPress is vulnerable to arbitrary file downloads and backup location writes in all versions up

## Risk And Classification

**Primary CVSS:** v3.1 3.8 LOW from security@wordfence.com

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

**EPSS:** 0.000340000 probability, percentile 0.099610000 (date 2026-04-08)

**Problem Types:** CWE-73 | CWE-73 CWE-73 External Control of File Name or Path

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	3.8	LOW	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N
3.1	CNA	DECLARED	3.8	LOW	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

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

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Backupbolt</a>	<a href="#">Backup Bolt</a>	affected 1.4.1 semver	Not specified

#### References

Reference	Source	Link
<a href="https://plugins.trac.wordpress.org/changeset">plugins.trac.wordpress.org/changeset</a>	<a href="mailto:security@wordfence.com">security@wordfence.com</a>	<a href="https://plugins.trac.wordpress.org/">plugins.trac.wordpress.org</a>
<a href="https://wordpress.org/plugins/backup-bolt">wordpress.org/plugins/backup-bolt</a>	<a href="mailto:security@wordfence.com">security@wordfence.com</a>	<a href="https://wordpress.org">wordpress.org</a>
<a href="https://www.wordfence.com/threat-intel/vulnerabilities/id/63f38644-a021-407a-9882-2c843...">www.wordfence.com/threat-intel/vulnerabilities/id/63f38644-a021-407a-9882-2c843...</a>	<a href="mailto:security@wordfence.com">security@wordfence.com</a>	<a href="https://www.wordfence.com">www.wordfence.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

#### Vendor Comments And Credit

Discovery Credit

**CNA:** Jonas Benjamin Friedli (en)

#### Additional Advisory Data

Source	Time	Event
CNA	2025-10-02T00:00:00.000Z	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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)