



CVE-2022-0633

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

Summary

CVE	CVE-2022-0633
State	PUBLIC
Assigner	contact@wpscan.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-17 19:15:00 UTC
Updated	2022-02-18 21:19:00 UTC
Description	The UpdraftPlus WordPress plugin Free before 1.22.3 and Premium before 2.22.3 do not properly validate a user has the r

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Updraftplus	Updraftplus	All	All	All	All
Application	Updraftplus	Updraftplus	All	All	All	All

References

Reference	Source	Link	Tags
WordPress UpdraftPlus 1.22.2 Backup Disclosure ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit, Third Party Ac
Severe Vulnerability Fixed In UpdraftPlus 1.22.3	MISC	jetpack.com	Exploit, Third Party Ac
UpdraftPlus security release - 1.22.3 / 2.22.3 - please upgrade - UpdraftPlus	CONFIRM	updraftplus.com	Release Notes, Vende
Attention Required! Cloudflare	MISC	wpscan.com	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Marc Montpas

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](#)