CVE-2020-12104

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

Summary

CVE	CVE-2020-12104
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-05-05 15:15:00 UTC
Updated	2020-05-07 20:16:00 UTC
Description	The Import feature in the wp-advanced-search plugin 3.3.6 for WordPress is vulnerable to authenticated SQL injection via a

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wp-advanced-search Project	Wp-advanced-search	All	All	All	All
Application	Wp-advanced-search Project	Wp-advanced-search	All	All	All	All

References

Reference	Source	Link	Tags
wordpress.org/plugins/wp-advanced-search	MISC	wordpress.org	Product, Third Party Advisc
WP-Advanced-Search < 3.3.7 - Authenticated SQL Injection Security Vulnerability	MISC	wpvulndb.com	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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