CVE-2016-6897

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

Summary

CVE	CVE-2016-6897
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-18 21:59:00 UTC
Updated	2017-09-03 01:29:00 UTC
Description	Cross-site request forgery (CSRF) vulnerability in the wp_ajax_update_plugin function in wp-admin/includes/ajax-actions.ph

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference
WordPress 4.5.3 - Authenticated Denial of Service (DoS)
oss-security - Path traversal vulnerability in WordPress Core Ajax handlers
Update/Install: Shiny Updates v2. · WordPress/WordPress@8c82515 · GitHub
WordPress CVE-2016-6897 Cross Site Request Forgery Vulnerability
WordPress Bugs Let Remote Users Conduct Cross-Site Request Forgery Attacks and Remote Authenticated Users Deny Service - SecurityTr
WordPress Core 4.5.3 - Directory Traversal / Denial of Service - PHP webapps Exploit
sumofpwn.nl/advisory/2016/path_traversal_vulnerability_in_wordpress_core_...
CVE Program record
NVD vulnerability detail

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