WordPress Plugin Thumbnail carousel slider Arbitrary File Upload (1.0)

Description

WordPress Plugin Thumbnail carousel slider is prone to a vulnerability that lets attackers upload arbitrary files because the application fails to properly verify user-supplied input. An attacker can exploit this vulnerability to upload arbitrary code and run it in the context of the webserver process. This may facilitate unauthorized access or privilege escalation; other attacks are also possible. WordPress Plugin Thumbnail carousel slider version 1.0 is vulnerable.

Remediation

Edit the source code to ensure that input is properly verified or disable the plugin until a fix is available

References

https://www.exploit-db.com/exploits/37998/ (https://www.exploit-db.com/exploits/37998/)

https://packetstormsecurity.com/files/133360/WordPress-Responsive-Thumbnail-Slider-1.0-Shell-Upload.html (https://packetstormsecurity.com/files/133360/WordPress-Responsive-Thumbnail-Slider-1.0-Shell-Upload.html)

https://www.pluginvulnerabilities.com/2016/07/26/wordpress-plugin-directorys-failure-to-enforce-developer-guidelines-puts-websites-at-risk/ (https://www.pluginvulnerabilities.com/2016/07/26/wordpress-plugin-directorys-failure-to-enforce-developer-guidelines-puts-websites-at-risk/)

Related Vulnerabilities

WordPress Plugin Recipes Writer Cross-Site Scripting (1.0.4) (https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-recipes-writer-cross-site-scripting-1-0-4/)

PHP Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability (CVE-2014-9427) (https://www.acunetix.com/vulnerabilities/web/php-improper-restriction-of-operations-within-the-bounds-of-a-memory-buffer-vulnerability-cve-2014-9427/)

WordPress Plugin WF Cookie Consent Cross-Site Scripting (1.1.3) (https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-wf-cookie-consent-cross-site-scripting-1-1-3/)

WordPress Plugin EZ SQL Reports Shortcode Widget and DB Backup Multiple Vulnerabilities (4.11.33) (https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-ez-sql-reports-shortcode-widget-and-db-backup-multiple-vulnerabilities-4-11-33/)

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability (CVE-2014-6071) (https://www.acunetix.com/vulnerabilities/web/jquery-improper-neutralization-of-input-during-web-page-generation-cross-site-scripting-vulnerability-cve-2014-6071/)

Severity

HIGH

Classification

CWE-434 (https://cwe.mitre.org/data/definitions/434.html)

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L
(https://www.first.org/cvss/calculator/3.0#CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L)

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N
(https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N)

Tags

Missing Update (https://www.acunetix.com/vulnerabilities/web/tag/missing-update/)

Unauthenticated File Upload (https://www.acunetix.com/vulnerabilities/web/tag/unauthenticated-file-upload/)

plans/)

scanner/web-application-security/)

traversal/)

Vulnerability Management Software (https://www.acunetix.com/vulnerability-scanner/vulnerability-management-software/)

LEARN MORE

White Papers (https://www.acunetix.com/white-papers/)

TLS Security (https://www.acunetix.com/blog/articles/tls-security-what-is-tls-ssl-part-1/)

WordPress Security (https://www.acunetix.com/vulnerability-scanner/wordpress-security-scan/)

Web Service Security (https://www.acunetix.com/websitesecurity/web-services-wp/)

Prevent SQL Injection (https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/)

COMPANY

About Us (https://www.acunetix.com/about/)

Customers (https://www.acunetix.com/vulnerability-scanner/customers/)

Become a Partner (https://www.acunetix.com/partners/)

Careers (https://www.acunetix.com/careers/)

Contact (https://www.acunetix.com/contact/)

DOCUMENTATION

Case Studies (https://www.acunetix.com/case-studies/)

Documentation (https://www.acunetix.com/support/)

Videos (https://www.acunetix.com/support/videos/)

Vulnerability Index (/vulnerabilities)

Webinars (https://www.acunetix.com/webinars/)

Login (https://online.acunetix.com)

Invicti Subscription Services Agreement (https://www.invicti.com/legal/ssa/)

Privacy Policy (https://www.invicti.com/legal/privacy-policy/)

Terms of Use (https://www.acunetix.com/about/terms_conditions/)

Sitemap (https://www.acunetix.com/sitemap/)