WordPress Plugin DELUCKS SEO Cross-Site Scripting (2.1.7)

Description

WordPress Plugin DELUCKS SEO is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input. An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks. WordPress Plugin DELUCKS SEO version 2.1.7 is vulnerable; prior versions may also be affected.

Remediation

Update to plugin version 2.1.9 or latest

References

https://www.pluginvulnerabilities.com/2019/09/21/hackers-may-already-be-targeting-this-persistent-xss-vulnerability-in-delucks-seo/ (https://www.pluginvulnerabilities.com/2019/09/21/hackers-may-already-be-targeting-this-persistent-xss-vulnerability-in-delucks-seo/)

https://blog.nintechnet.com/vulnerability-in-the-wordpress-delucks-seo-plugin-actively-exploited/ (https://blog.nintechnet.com/vulnerability-in-the-wordpress-delucks-seo-plugin-actively-exploited/)

https://delucks.com/en/wordpress-seo-plugin/information-about-the-hack/ (https://delucks.com/en/wordpress-seo-plugin/information-about-the-hack/)

https://plugins.trac.wordpress.org/changeset?old_path=%2Fdelucks-seo&old=2099783&new_path=%2Fdelucks-seo&new=2161211&sfp_email=&sfph_mail= (https://plugins.trac.wordpress.org/changeset?old_path=%2Fdelucks-seo&old=2099783&new_path=%2Fdelucks-seo&new=2161211&sfp_email=&sfph_mail=)

Related Vulnerabilities

Oracle JRE CVE-2013-2422 Vulnerability (CVE-2013-2422) (https://www.acunetix.com/vulnerabilities/web/oracle-jre-cve-2013-2422-vulnerability-cve-2013-2422/)

WordPress Plugin Download Plugin Unspecified Vulnerability (1.6.1) (https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-download-plugin-unspecified-vulnerability-1-6-1/)

WordPress 4.2.x Same Origin Method Execution (SOME) Vulnerability (4.2 - 4.2.7) (https://www.acunetix.com/vulnerabilities/web/wordpress-4-2-x-same-origin-method-execution-some-vulnerability-4-2-4-2-7/)

WordPress Plugin WP Review Slider SQL Injection (10.9) (https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-wp-review-slider-sql-injection-10-9/)

ZenCart Exposure of Sensitive Information to an Unauthorized Actor Vulnerability (CVE-2009-4322) (https://www.acunetix.com/vulnerabilities/web/zencart-exposure-of-sensitive-information-to-an-unauthorized-actor-vulnerability-cve-2009-4322/)

Severity

HIGH

Classification

CWE-79 (https://cwe.mitre.org/data/definitions/79.html)

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

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

Tags

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

XSS (https://www.acunetix.com/vulnerabilities/web/tag/xss/)

scanner/acunetix-integrations/)

Vulnerability Scanner (/vulnerability-scanner/)

Support Plans (https://www.acunetix.com/support-plans/)

External Vulnerability Scanner (https://www.acunetix.com/vulnerability-scanner/external-vulnerability-scanner/)

Web Application Security (https://www.acunetix.com/vulnerability-scanner/web-application-security/)

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

CSRF Attacks (https://www.acunetix.com/websitesecurity/c attacks/)

Directory Traversal (https://www.acunetix.com/websitesecurity/c traversal/)

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/)