

[WEB APPLICATION VULNERABILITIES \(/VULNERABILITIES/\)](#) > [STANDARD & PREMIUM \(/VULNERABILITIES/WEB/\)](#)

WordPress Plugin MainWP Dashboard Cross-Site Scripting (3.1.2)

Description

WordPress Plugin MainWP Dashboard 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 MainWP Dashboard version 3.1.2 is vulnerable; prior versions may also be affected.

Remediation

Update to plugin version 3.1.3 or latest

References

<https://klikki.fi/adv/mainwp.html> (<https://klikki.fi/adv/mainwp.html>)

<https://wordpress.org/plugins/mainwp/changelog/> (<https://wordpress.org/plugins/mainwp/changelog/>)

Related Vulnerabilities

[WordPress 4.2.x Multiple Vulnerabilities \(4.2 - 4.2.27\)](https://www.acunetix.com/vulnerabilities/web/wordpress-4-2-x-multiple-vulnerabilities-4-2-4-2-27/) (<https://www.acunetix.com/vulnerabilities/web/wordpress-4-2-x-multiple-vulnerabilities-4-2-4-2-27/>)

[Artifactory Incorrect Permission Assignment for Critical Resource Vulnerability \(CVE-2021-41834\)](https://www.acunetix.com/vulnerabilities/web/artifactory-incorrect-permission-assignment-for-critical-resource-vulnerability-cve-2021-41834/) (<https://www.acunetix.com/vulnerabilities/web/artifactory-incorrect-permission-assignment-for-critical-resource-vulnerability-cve-2021-41834/>)

[WordPress Plugin Duplicate Page and Post Spam Injection \(2.1\)](https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-duplicate-page-and-post-spam-injection-2-1-1/) (<https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-duplicate-page-and-post-spam-injection-2-1-1/>)

[WordPress Plugin spideranalyse Cross-Site Scripting \(0.0.1\)](https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-spideranalyse-cross-site-scripting-0-0-1/) (<https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-spideranalyse-cross-site-scripting-0-0-1/>)

[Oracle JRE CVE-2012-3216 Vulnerability \(CVE-2012-3216\)](https://www.acunetix.com/vulnerabilities/web/oracle-jre-cve-2012-3216-vulnerability-cve-2012-3216/) (<https://www.acunetix.com/vulnerabilities/web/oracle-jre-cve-2012-3216-vulnerability-cve-2012-3216/>)

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/>)

Take action and discover your vulnerabilities

[Get a demo \(https://www.acunetix.com/web-vulnerability-scanner/demo/\)](https://www.acunetix.com/web-vulnerability-scanner/demo/)



GARMIN



Cognizant



U.S. AIR FORCE



PRODUCT INFORMATION

[AcuSensor Technology
\(https://www.acunetix.com/vulnerability-scanner/acusensor-technology/\)](https://www.acunetix.com/vulnerability-scanner/acusensor-technology/)

[AcuMonitor Technology
\(https://www.acunetix.com/vulnerability-scanner/acumonitor-technology/\)](https://www.acunetix.com/vulnerability-scanner/acumonitor-technology/)

[Acunetix Integrations
\(https://www.acunetix.com/vulnerability-scanner/acunetix-integrations/\)](https://www.acunetix.com/vulnerability-scanner/acunetix-integrations/)

[Vulnerability Scanner \(/vulnerability-scanner/\)](https://www.acunetix.com/vulnerability-scanner/)

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

USE CASES

[Penetration Testing Software
\(https://www.acunetix.com/vulnerability-scanner/penetration-testing-software/\)](https://www.acunetix.com/vulnerability-scanner/penetration-testing-software/)

[Website Security Scanner
\(https://www.acunetix.com/vulnerability-scanner/website-security-scanner/\)](https://www.acunetix.com/vulnerability-scanner/website-security-scanner/)

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

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

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

WEBSITE SECURITY

[Cross-site Scripting
\(https://www.acunetix.com/websitesecurity/cross-site-scripting/\)](https://www.acunetix.com/websitesecurity/cross-site-scripting/)

[SQL Injection
\(https://www.acunetix.com/websitesecurity/sql-injection/\)](https://www.acunetix.com/websitesecurity/sql-injection/)

[Reflected XSS
\(https://www.acunetix.com/websitesecurity/reflective-xss/\)](https://www.acunetix.com/websitesecurity/reflective-xss/)

[CSRF Attacks
\(https://www.acunetix.com/websitesecurity/csrf-attacks/\)](https://www.acunetix.com/websitesecurity/csrf-attacks/)

[Directory Traversal
\(https://www.acunetix.com/websitesecurity/directory-traversal/\)](https://www.acunetix.com/websitesecurity/directory-traversal/)

LEARN MORE[White Papers](https://www.acunetix.com/white-papers/)

(<https://www.acunetix.com/white-papers/>).

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

(<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/)

(<https://www.acunetix.com/vulnerability-scanner/wordpress-security-scan/>).

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

(<https://www.acunetix.com/websitesecurity/web-services-wp/>).

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

(<https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/>).

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

(<https://www.acunetix.com/about/>).

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

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

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

(<https://www.acunetix.com/partners/>).

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

(<https://www.acunetix.com/careers/>).

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

(<https://www.acunetix.com/contact/>).

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

(<https://www.acunetix.com/case-studies/>).

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

(<https://www.acunetix.com/support/>).

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

(<https://www.acunetix.com/support/videos/>).

[Vulnerability Index \(/vulnerabilities\)](/vulnerabilities)

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

(<https://www.acunetix.com/webinars/>).

[Login \(https://online.acunetix.com\)](https://online.acunetix.com)

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

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

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

[Sitemap \(https://www.acunetix.com/sitemap/\)](https://www.acunetix.com/sitemap/)

© Acunetix 2026, by Invicti (<https://www.acunetix.com>)