

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

WordPress Plugin N-Media Website Contact Form with File Upload Arbitrary File Upload (1.3.4)

Description

WordPress Plugin N-Media Website Contact Form with File Upload is prone to a vulnerability that lets attackers upload arbitrary files because the application fails to properly sanitize 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 N-Media Website Contact Form with File Upload version 1.3.4 is vulnerable; prior versions may also be affected.

Remediation

Update to plugin version 1.4 or latest

References

<https://www.homelab.it/index.php/2015/04/12/wordpress-n-media-website-contact-form-shell-upload/>
(<https://www.homelab.it/index.php/2015/04/12/wordpress-n-media-website-contact-form-shell-upload/>)

<http://www.exploit-db.com/exploits/36738/> (<https://www.exploit-db.com/exploits/36738/>)

<http://packetstormsecurity.com/files/131413/WordPress-N-Media-Website-Contact-Form-1.3.4-Shell-Upload.html>
(<http://packetstormsecurity.com/files/131413/WordPress-N-Media-Website-Contact-Form-1.3.4-Shell-Upload.html>)

<http://packetstormsecurity.com/files/131514/WordPress-N-Media-Website-Contact-Form-Upload.html>
(<http://packetstormsecurity.com/files/131514/WordPress-N-Media-Website-Contact-Form-Upload.html>)

https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/webapp/wp_nmediawebsite_file_upload.rb
(https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/webapp/wp_nmediawebsite_file_upload.rb)

<https://www.exploit-db.com/exploits/36979/> (<https://www.exploit-db.com/exploits/36979/>)

Related Vulnerabilities

[MySQL CVE-2020-14643 Vulnerability \(CVE-2020-14643\)](#) (<https://www.acunetix.com/vulnerabilities/web/mysql-cve-2020-14643-vulnerability-cve-2020-14643/>)

[Zope Web Application Server Improper Limitation of a Pathname to a Restricted Directory \('Path Traversal'\) Vulnerability \(CVE-2021-32674\)](#) (<https://www.acunetix.com/vulnerabilities/web/zope-web-application-server-improper-limitation-of-a-pathname-to-a-restricted-directory-path-traversal-vulnerability-cve-2021-32674/>)

[WordPress Plugin Image Slider Cross-Site Scripting \(1.1.5\) \(https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-image-slider-cross-site-scripting-1-1-5/\)](https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-image-slider-cross-site-scripting-1-1-5/)

[Oracle Database Server Improper Neutralization of Special Elements used in an SQL Command \('SQL Injection'\) Vulnerability \(CVE-2007-5511\) \(https://www.acunetix.com/vulnerabilities/web/oracle-database-server-improper-neutralization-of-special-elements-used-in-an-sql-command-sql-injection-vulnerability-cve-2007-5511/\)](https://www.acunetix.com/vulnerabilities/web/oracle-database-server-improper-neutralization-of-special-elements-used-in-an-sql-command-sql-injection-vulnerability-cve-2007-5511/)

[Apache Tomcat Improper Input Validation Vulnerability \(CVE-2016-3092\) \(https://www.acunetix.com/vulnerabilities/web/apache-tomcat-improper-input-validation-vulnerability-cve-2016-3092/\)](https://www.acunetix.com/vulnerabilities/web/apache-tomcat-improper-input-validation-vulnerability-cve-2016-3092/)

Severity

HIGH

Classification

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

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

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/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:N/VC:H/VI:H/VA:H/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/>)

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/)



[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/>)

[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/>)

[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/reflected-xss/)
(<https://www.acunetix.com/websitesecurity/reflected-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 \(/vulnerabilities\)](https://www.acunetix.com/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>)