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

Drupal Core 5.x Cross-Site Request Forgery (5.0 - 5.2) (https://www.acunetix.com/vulnerabilities/web/drupal-core-5-x-cross-site-request-forgery-5-0-5-2/)

WordPress Plugin Custom Field Template PHP Object Injection (2.5.7) (https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-custom-field-template-php-object-injection-2-5-7/)

MySQL CVE-2016-0610 Vulnerability (CVE-2016-0610) (https://www.acunetix.com/vulnerabilities/web/mysql-cve-2016-0610-vulnerability-cve-2016-0610/)

WordPress Plugin weForms-Easy Drag & Drop Contact Form Builder For WordPress Unspecified Vulnerability (1.5.3) (https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-weforms-easy-drag-drop-contact-form-builder-for-wordpress-unspecified-vulnerability-1-5-3/)

MySQL CVE-2015-0411 Vulnerability (CVE-2015-0411) (https://www.acunetix.com/vulnerabilities/web/mysql-cve-2015-0411-vulnerability-cve-2015-0411/)

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/)

scanner/acusensor-technology/)

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

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

Vulnerability Scanner (/vulnerability-scanner/)

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

scanner/penetration-testing-software/)

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

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

site-scripting/)

SQL Injection (https://www.acunetix.com/websitesecurity/sinjection/)

Reflected XSS (https://www.acunetix.com/websitesecurity/x

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

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

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/)