

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

WordPress Plugin Work The Flow File Upload Arbitrary File Upload (2.5.2)

Description

WordPress Plugin Work The Flow 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 Work The Flow File Upload version 2.5.2 is vulnerable; prior versions may also be affected.

Remediation

Update to plugin version 2.5.3 or latest

References

<https://www.homelab.it/index.php/2015/04/04/wordpress-work-the-flow-file-upload-vulnerability/>
(<https://www.homelab.it/index.php/2015/04/04/wordpress-work-the-flow-file-upload-vulnerability/>)

<https://www.exploit-db.com/exploits/36640/> (<https://www.exploit-db.com/exploits/36640/>)

<http://packetstormsecurity.com/files/131294/WordPress-Work-The-Flow-2.5.2-Shell-Upload.html>
(<http://packetstormsecurity.com/files/131294/WordPress-Work-The-Flow-2.5.2-Shell-Upload.html>)

<http://packetstormsecurity.com/files/131512/WordPress-Work-The-Flow-Upload.html>
(<http://packetstormsecurity.com/files/131512/WordPress-Work-The-Flow-Upload.html>)

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

Related Vulnerabilities

[TCExam Improper Neutralization of Special Elements used in an SQL Command \('SQL Injection'\) Vulnerability \(CVE-2012-4601\)](https://www.acunetix.com/vulnerabilities/web/tcexam-improper-neutralization-of-special-elements-used-in-an-sql-command-sql-injection-vulnerability-cve-2012-4601/) (<https://www.acunetix.com/vulnerabilities/web/tcexam-improper-neutralization-of-special-elements-used-in-an-sql-command-sql-injection-vulnerability-cve-2012-4601/>)

[WordPress Plugin IMPress for IDX Broker Unspecified Vulnerability \(2.5.11\)](https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-impress-for-idx-broker-unspecified-vulnerability-2-5-11/) (<https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-impress-for-idx-broker-unspecified-vulnerability-2-5-11/>)

[WebLogic CVE-2017-10352 Vulnerability \(CVE-2017-10352\)](https://www.acunetix.com/vulnerabilities/web/weblogic-cve-2017-10352-vulnerability-cve-2017-10352/) (<https://www.acunetix.com/vulnerabilities/web/weblogic-cve-2017-10352-vulnerability-cve-2017-10352/>)

WordPress Plugin Users Ultra Membership Cross-Site Scripting (1.5.78) (<https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-users-ultra-membership-cross-site-scripting-1-5-78/>)

ATutor Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') Vulnerability (CVE-2016-10400) (<https://www.acunetix.com/vulnerabilities/web/atutor-improper-limitation-of-a-pathname-to-a-restricted-directory-path-traversal-vulnerability-cve-2016-10400/>)

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/)



Cognizant

GARMIN



PRODUCT INFORMATION

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

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

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

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

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

[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/>)

[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](https://www.acunetix.com/vulnerabilities/) ([/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/>)