

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

# WordPress Plugin Thumbnail carousel slider Arbitrary File Upload (1.0)

## Description

WordPress Plugin Thumbnail carousel slider is prone to a vulnerability that lets attackers upload arbitrary files because the application fails to properly verify 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 Thumbnail carousel slider version 1.0 is vulnerable.

## Remediation

Edit the source code to ensure that input is properly verified or disable the plugin until a fix is available

## References

<https://www.exploit-db.com/exploits/37998/> (<https://www.exploit-db.com/exploits/37998/>)

---

<https://packetstormsecurity.com/files/133360/WordPress-Responsive-Thumbnail-Slider-1.0-Shell-Upload.html>  
(<https://packetstormsecurity.com/files/133360/WordPress-Responsive-Thumbnail-Slider-1.0-Shell-Upload.html>)

---

<https://www.pluginvulnerabilities.com/2016/07/26/wordpress-plugin-directorys-failure-to-enforce-developer-guidelines-puts-websites-at-risk/> (<https://www.pluginvulnerabilities.com/2016/07/26/wordpress-plugin-directorys-failure-to-enforce-developer-guidelines-puts-websites-at-risk/>)

---

## Related Vulnerabilities

[WordPress Plugin LOGOSWARE SUITE Uploader Arbitrary File Upload \(1.1.6\)](https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-logosware-suite-uploader-arbitrary-file-upload-1-1-6/)  
(<https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-logosware-suite-uploader-arbitrary-file-upload-1-1-6/>)

---

[Craft CMS Improper Neutralization of Input During Web Page Generation \('Cross-site Scripting'\) Vulnerability \(CVE-2023-30177\)](https://www.acunetix.com/vulnerabilities/web/craft-cms-improper-neutralization-of-input-during-web-page-generation-cross-site-scripting-vulnerability-cve-2023-30177/)  
(<https://www.acunetix.com/vulnerabilities/web/craft-cms-improper-neutralization-of-input-during-web-page-generation-cross-site-scripting-vulnerability-cve-2023-30177/>)

---

[WordPress Plugin LeagueManager Multiple SQL Injection Vulnerabilities \(3.9.1.1\)](https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-leaguemanager-multiple-sql-injection-vulnerabilities-3-9-1-1/)  
(<https://www.acunetix.com/vulnerabilities/web/wordpress-plugin-leaguemanager-multiple-sql-injection-vulnerabilities-3-9-1-1/>)

---

[MySQL CVE-2020-2790 Vulnerability \(CVE-2020-2790\)](https://www.acunetix.com/vulnerabilities/web/mysql-cve-2020-2790-vulnerability-cve-2020-2790/) (<https://www.acunetix.com/vulnerabilities/web/mysql-cve-2020-2790-vulnerability-cve-2020-2790/>)

---

[GibbonEdu Session Fixation Vulnerability \(CVE-2022-27305\)](https://www.acunetix.com/vulnerabilities/web/gibbonedu-session-fixation-vulnerability-cve-2022-27305/)  
(<https://www.acunetix.com/vulnerabilities/web/gibbonedu-session-fixation-vulnerability-cve-2022-27305/>)

---

## Severity

HIGH

## Classification

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

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

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

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

### 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-)  
([### WEBSITE SECURITY](https://www.acunetix.com/vulnerability-</a></p></div>
<div data-bbox=)

[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/>)

[plans/](#)

[scanner/web-application-security/](#)

[traversal/](#)

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

**LEARN MORE**

**COMPANY**

**DOCUMENTATION**

[White Papers](#)

[About Us](#)

[Case Studies](#)

[\(https://www.acunetix.com/white-papers/\)](https://www.acunetix.com/white-papers/)

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

[\(https://www.acunetix.com/case-studies/\)](https://www.acunetix.com/case-studies/)

[TLS Security](#)

[Customers](#)

[Documentation](#)

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

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

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

[WordPress Security](#)

[Become a Partner](#)

[Videos](#)

[\(https://www.acunetix.com/vulnerability-scanner/wordpress-security-scan/\)](https://www.acunetix.com/vulnerability-scanner/wordpress-security-scan/)

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

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

[Careers](#)

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

[Web Service Security](#)

[Contact](#)

[Webinars](#)

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

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

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

[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/)

[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>)