



# CVE-2022-40700

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2022-40700
<b>State</b>	RESERVED
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-01-19 15:15:00 UTC
<b>Updated</b>	2024-01-30 23:03:00 UTC
<b>Description</b>	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new

## Risk And Classification

**Problem Types: CWE-918**

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Agence-press</a>	<a href="#">Css Adder</a>	All	All	All	All
Application	<a href="#">Arcstone</a>	<a href="#">Amo For Wp - Membership Management</a>	All	All	All	All
Application	<a href="#">Deano</a>	<a href="#">Amp Toolbox</a>	All	All	All	All
Application	<a href="#">Designmodo</a>	<a href="#">Qards</a>	All	All	All	All
Application	<a href="#">Frumph</a>	<a href="#">Phpfreechat</a>	All	All	All	All
Application	<a href="#">Longwatchstudio</a>	<a href="#">Woosupply</a>	All	All	All	All
Application	<a href="#">Longwatchstudio</a>	<a href="#">Woovip</a>	All	All	All	All
Application	<a href="#">Longwatchstudio</a>	<a href="#">Woovirtualwallet</a>	All	All	All	All
Application	<a href="#">Millionclues</a>	<a href="#">Admin Css Mu</a>	All	All	All	All
Application	<a href="#">Millionclues</a>	<a href="#">Custom Login Admin Front-end Css</a>	All	All	All	All
Application	<a href="#">Montonio</a>	<a href="#">Montonio For Woocommerce</a>	All	All	All	All
Application	<a href="#">Paulclark</a>	<a href="#">Styles</a>	All	All	All	All
Application	<a href="#">Squidesma</a>	<a href="#">Theme Minifier</a>	All	All	All	All
Application	<a href="#">Unihost</a>	<a href="#">Confirm Data</a>	All	All	All	All
Application	<a href="#">Wpopal</a>	<a href="#">Wpopal Core Features</a>	All	All	All	All

## References

Reference	Source	Link
WordPress Custom Login Admin Front-end CSS plugin <= 1.4.1 - Server Side Request Forgery (SSRF) - Patchstack		<a href="#">patchstack</a>
WordPress WooSupply plugin <= 1.2.2 - Server Side Request Forgery (SSRF) - Patchstack		<a href="#">patchstack</a>
WordPress AMO for WP plugin <= 4.6.6 - Server Side Request Forgery (SSRF) - Patchstack		<a href="#">patchstack</a>
WordPress WooVirtualWallet plugin <= 2.2.1 - Server Side Request Forgery (SSRF) - Patchstack		<a href="#">patchstack</a>
WordPress AMP Toolbox plugin <= 2.1.1 - Server Side Request Forgery (SSRF) - Patchstack		<a href="#">patchstack</a>
WordPress Admin CSS MU plugin <= 2.6 - Server-Side Request Forgery (SSRF) vulnerability - Patchstack		<a href="#">patchstack</a>
WordPress WooVIP plugin <= 1.4.4 - Server Side Request Forgery (SSRF) - Patchstack		<a href="#">patchstack</a>
WordPress Styles plugin <= 1.2.3 - Server Side Request Forgery (SSRF) - Patchstack		<a href="#">patchstack</a>
WordPress Wpopal Core Features plugin <= 1.5.8 - Server Side Request Forgery (SSRF) - Patchstack		<a href="#">patchstack</a>
WordPress CSS Adder By Agene-Press plugin <= 1.5.0 - Server Side Request Forgery (SSRF) - Patchstack		<a href="#">patchstack</a>
WordPress Montonio for WooCommerce plugin <= 6.0.1 - Server Side Request Forgery (SSRF) - Patchstack		<a href="#">patchstack</a>
WordPress Confirm Data plugin <= 1.0.7 - Unauth. Server-Side Request Forgery (SSRF) vulnerability - Patchstack		<a href="#">patchstack</a>
WordPress WordPress Page Builder - Qards plugin <= 1.0.5 - Server Side Request Forgery (SSRF) - Patchstack		<a href="#">patchstack</a>
WordPress PHPFreeChat plugin <= 0.2.8 - Server Side Request Forgery (SSRF) - Patchstack		<a href="#">patchstack</a>
WordPress Theme Minifier plugin <= 2.0 - Server Side Request Forgery (SSRF) - Patchstack		<a href="#">patchstack</a>
CVE Program record	CVE.ORG	<a href="#">www.cve</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.g</a>

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**