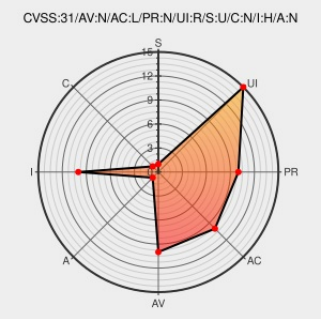
CVE-2015-9408

Published on: 09/20/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:21 PM UTC

CVE-2015-9408

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Xpinner Lite from Cyberseo contain the following vulnerability:

The xpinner-lite plugin through 2.2 for WordPress has wp-admin/options-general.php CSRF with resultant XSS.

CVE-2015-9408 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
WordPress xPinner Lite 2.2 Cross Site Request Forgery / Cross Site Scripting ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/133593/

xPinner Lite – WordPress plugin | WordPress.org	Product Third Party Advisory wordpress.org text/html	MISC wordpress.org/plugins/xpinner-lite/#developers
xPinner Lite <= 2.2 - Cross-Site Scripting (XSS) & CSRF	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC wpvulndb.com/vulnerabilities/8194

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cyberseo	Xpinner Lite	All	All	All	All

cpe:2.3:a:cyberseo:xpinner_lite:*:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→