



CVE-2021-36877

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

Summary

CVE	CVE-2021-36877
State	PUBLIC
Assigner	audit@patchstack.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-27 16:15:00 UTC
Updated	2021-10-01 02:13:00 UTC
Description	Cross-Site Request Forgery (CSRF) vulnerability in WordPress uListing plugin (versions <= 2.0.5) makes it possible for att

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Stylemixthemes	Ulisting	All	All	All	All

References

Reference	Source	Link
WordPress uListing plugin <= 2.0.5 - Modify User Roles via Cross-Site Request Forgery (CSRF) vulnerability - Patchstack	MISC	patc
Listing, Classified Ads & Business Directory – uListing – WordPress plugin WordPress.org	CONFIRM	wor
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd.

Vendor Comments And Credit

Discovery Credit

LEGACY: Original researcher - m0ze (Patchstack Red Team)

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

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](#)