



CVE-2020-5530

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

Summary

CVE	CVE-2020-5530
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-18 06:15:00 UTC
Updated	2020-02-19 14:25:00 UTC
Description	Cross-site request forgery (CSRF) vulnerability in Easy Property Listings versions prior to 3.4 allows remote attackers to hijack sessions of authenticated users.

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Realestateconnected	Easy Property Listings	All	All	All	All
Application	Realestateconnected	Easy Property Listings	All	All	All	All

References

Reference	Source	Link	Tags
Easy Property Listings < 3.4 - Cross-Site Request Forgery (CSRF) Security Vulnerability	MISC	wpvulndb.com	Third Party
JVN#89259622: WordPress Plugin "Easy Property Listings" vulnerable to cross-site request forgery	MISC	jvn.jp	Third Party
WordPress › Easy Property Listings « WordPress Plugins	MISC	wordpress.org	Release Information
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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](#).

Free CVE JSON API [cve.report/api](#)

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