



CVE-2018-19135

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

Summary

CVE	CVE-2018-19135
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-11-11 04:29:00 UTC
Updated	2019-01-30 15:40:00 UTC
Description	ClipperCMS 1.3.3 does not have CSRF protection on its kcfinder file upload (enabled by default). This can be used by an a

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Clippercms	Clippercms	1.3.3	All	All	All
Application	Clippercms	Clippercms	1.3.3	All	All	All

References

Reference	Source	Link	T
ClipperCMS 1.3.3 File Upload CSRF Vulnerability · Issue #494 · ClipperCMS/ClipperCMS · GitHub	MISC	github.com	E
ClipperCMS 1.3.3 - Cross-Site Request Forgery (File Upload) - PHP webapps Exploit	EXPLOIT-DB	www.exploit-db.com	E
CVE Program record	CVE.ORG	www.cve.org	cc
NVD vulnerability detail	NVD	nvd.nist.gov	cc

No vendor comments have been submitted for this CVE.

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

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