



CVE-2019-11537

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

Summary

CVE	CVE-2019-11537
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-04-25 19:29:00 UTC
Updated	2019-05-07 18:57:00 UTC
Description	In osTicket before 1.12, XSS exists via /upload/file.php, /upload/scp/users.php?do=import-users, and /upload/scp/ajax.php/

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Osticket	Osticket	All	All	All	All
Application	Osticket	Osticket	All	All	All	All

References

Reference	Source	Link	Tags
osTicket 1.11 - Cross-Site Scripting / Local File Inclusion - PHP webapps Exploit	EXPLOIT-DB	www.exploit-db.com	Exploit, T
xss: XSS To LFI Vulnerability by JediKev · Pull Request #4869 · osTicket/osTicket · GitHub	MISC	github.com	Third Par
osTicket 1.11 - Cross-Site Scripting / Local File Inclusion - PHP webapps Exploit	MISC	www.exploit-db.com	Exploit, T
Release v1.12 · osTicket/osTicket · GitHub	MISC	github.com	Third Par
Pentest Blog - Self-Improvement to Ethical Hacking	MISC	pentest.com.tr	Exploit, T
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

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](#).

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

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