



CVE-2020-24917

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

Summary

CVE	CVE-2020-24917
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-08-30 16:15:00 UTC
Updated	2020-09-03 18:19:00 UTC
Description	osTicket before 1.14.3 allows XSS via a crafted filename to DraftAjaxAPI::_uploadInlineImage() in include/ajax.draft.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
xss: Draft Uploaded Attachment · osTicket/osTicket@518de22 · GitHub	MISC	github.c
Cross site scripting in OsTicket (CVE-2020-24917) Systems & Internet Security Lab University of Illinois at Chicago	MISC	sisl.lab.i
Comparing v1.14.2...v1.14.3 · osTicket/osTicket · GitHub	MISC	github.c
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

No vendor comments have been submitted for this CVE.

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

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