



CVE-2021-36787

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

Summary

CVE	CVE-2021-36787
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-13 17:15:00 UTC
Updated	2022-02-10 07:44:00 UTC
Description	The femanager extension before 5.5.1 and 6.x before 6.3.1 for TYPO3 allows XSS via a crafted SVG document.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Femanager Project	Femanager	All	All	All	All
Application	In2code	Femanager	All	All	All	All

References

Reference	Source	Link
Full Disclosure: SEC Consult SA-20220117-0 :: Stored Cross-Site Scripting vulnerability in TYPO3 extension "femanager"	FULLDISC	sec
TYPO3 femanager 6.3.0 Cross Site Scripting ~ Packet Storm	MISC	pac
TYPO3 Security Bulletins	MISC	typo
TYPO3-EXT-SA-2021-010: Cross-Site Scripting in Extension "femanager" (femanager)	CONFIRM	typo
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd

No vendor comments have been submitted for this CVE.

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

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