



CVE-2020-14294

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

Summary

CVE	CVE-2020-14294
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-02 09:15:00 UTC
Updated	2020-10-08 00:44:00 UTC
Description	An issue was discovered in Secudos Qiata FTA 1.70.19. The comment feature allows persistent XSS that is executed when

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Secudos	Qiata Fta	All	All	All	All

References

Reference	Source	Link	Tag
www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2020-024.txt	MISC	www.syss.de	Exploit
SYSS-2020-024 und SYSS-2020-025: Zwei Schwachstellen in File Transfer-Lösung Qiata von Secudos	MISC	www.syss.de	Threat
Full Disclosure: [SYSS-2020-024] Qiata FTA - Persistent Cross-Site Scripting	MISC	seclists.org	Exploit
Index of /	MISC	www.qiata.com	Product
GitHub - patrickhener/CVE-2020-14294: This repository holds the advisory of the CVE-2020-14294	MISC	github.com	Threat
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.

© [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](#)