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 wher

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	Expl
SYSS-2020-024 und SYSS-2020-025: Zwei Schwachstellen in File Transfer-Lösung Qiata von Secudos	MISC	www.syss.de	Thir
Full Disclosure: [SYSS-2020-024] Qiata FTA - Persistent Cross-Site Scripting	MISC	seclists.org	Expl
Index of /	MISC	www.qiata.com	Proc
GitHub - patrickhener/CVE-2020-14294: This repository holds the advisory of the CVE-2020-14294	MISC	github.com	Thir
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report