CVE-2021-38542

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2021-38542
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-04 09:15:00 UTC
Updated	2022-10-27 11:39:00 UTC
Description	Apache James prior to release 3.6.1 is vulnerable to a buffering attack relying on the use of the STARTTLS command. This

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	James	All	All	All	All

References

Reference	Source	Link
oss-security - CVE-2021-38542: Apache James vulnerable to STARTTLS command injection (IMAP and POP3)	MLIST	www.openwall
oss-security - CVE-2022-28220: STARTTLS command injection in Apache JAMES	MLIST	www.openwall
oss-security - CVE-2021-38542: Apache James vulnerable to STARTTLS command injection (IMAP and POP3)	MISC	www.openwall
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: We thanks Benoit Tellier, Raphael Ouazana for reporting this vulnerability as well as Damian Poddebniak, Fabian Ising, Hanno Böck, and Sebastian Schinzel Münster University of Applied Science for their research and tools regarding STARTTLS security.

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