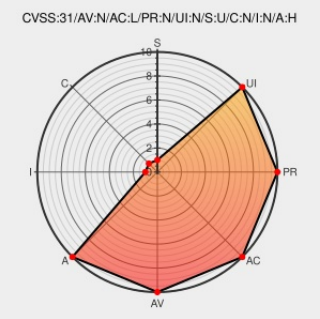
CVE-2022-28220

Published on: Not Yet Published

Last Modified on: 09/30/2022 07:16:00 PM UTC

CVE-2022-28220

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of James from Apache contain the following vulnerability:

Apache James prior to release 3.6.3 and 3.7.1 is vulnerable to a buffering attack relying on the use of the STARTTLS command. Fix of CVE-2021-38542, which solved similar problem fron Apache James 3.6.1, is subject to a parser differential and do not take into account concurrent requests.

CVE-2022-28220 has been assigned by security@apache.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Apache Software Foundation** - **Apache James** version **<= 3.6.2**

Affected Vendor/Software: **Apache Software Foundation** - **Apache James** version **<= 3.7.0**

Vulnerability Patch/Work Around

Upgrade to Apache James 3.7.1 or Apache James 3.6.3.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVE References

Description	Tags	Link
Apache James	james.apache.org text/html	MISC james.apache.org/james/update/2022/08/26/james-3.7.1.html
oss-security - CVE-2022-28220: STARTTLS command injection in Apache JAMES	www.openwall.com text/html	MLIST [oss-security] 20220919 CVE-2022-28220: STARTTLS command injection in Apache JAMES

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Apache James prior to release 3.6.3 and 3.7.1 is vulnerable to a buffering attack relying on the use of the STARTTLS …

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	James	3.7.0	All	All	All
Application	Apache	James	All	All	All	All

cpe:2.3:a:apache:james:3.7.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:james:*:*:*:*:*:*:*:*:

Discovery Credit

Apache James PMC would like to thanks Benoit TELLIER for this report, and Fabian Ising for his support.

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-28220 : #Apache James prior to release 3.6.3 and 3.7.1 is vulnerable to a buffering attack relying on the… twitter.com/i/web/status/1…	2022-09-08 07:46:33
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-28220 Apache James prior to release 3.6.3 and 3.7.1 is vulnerable to a… twitter.com/i/web/status/1…	2022-09-08 09:56:00
/r/netcve	CVE-2022-28220	2022-09-08 08:38:32

← Previous ID

Next ID→

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