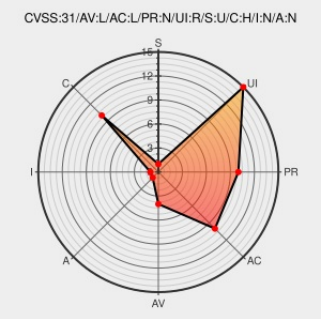
CVE-2022-27875

Published on: Not Yet Published

Last Modified on: 05/12/2022 08:48:00 PM UTC

CVE-2022-27875

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



Certain versions of Access For Android from F5 contain the following vulnerability:

On F5 Access for Android 3.x versions prior to 3.0.8, a Task Hijacking vulnerability exists in the F5 Access for Android application, which may allow an attacker to steal sensitive user information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated

CVE-2022-27875 has been assigned by f5sirt@f5.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **F5** - **F5 Access for Android** version **< 3.0.8**

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
No Description Provided	support.f5.com	MISC support.f5.com/csp/article/K40019131

text/html

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.

Related QID Numbers

376690 F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) F5 Access for Android vulnerability (K40019131)

630815 F5 Access For Android Exposure of Sensitive Information Vulnerability

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	Access For Android	All	All	All	All

cpe:2.3:a:f5:access_for_android:*:*:*:*:*:*:*:*:

Discovery Credit

F5 acknowledges Sheikh Rishad for bringing this issue to our attention and following the highest standards of coordinated disclosure.

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-27875 : On F5 Access for Android 3.x versions prior to 3.0.8, a Task Hijacking vulnerability exists in the… twitter.com/i/web/status/1…	2022-05-05 17:13:37
/r/k12cybersecurity	MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in F5Networks Products Could Allow for Arbitrary Code Execution - PATCH: NOW	2022-05-06 14:11:01
/r/k12cybersecurity	UPDATED MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in F5Networks Products Could Allow for Arbitrary Code Execution - PATCH: NOW	2022-05-09 13:34:10
/r/k12cybersecurity	UPDATED MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in F5Networks Products Could Allow for Arbitrary Code Execution - PATCH: NOW	2022-05-11 16:42:45

← Previous ID

Next ID→