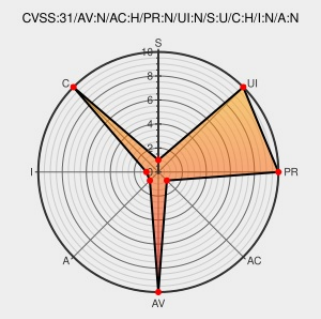
CVE-2020-15047

Published on: 06/25/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:41 PM UTC

CVE-2020-15047

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



Certain versions of Trojita from Trojita Project contain the following vulnerability:

MSA/SMTP.cpp in Trojita before 0.8 ignores certificate-verification errors, which allows man-in-the-middle attackers to spoof SMTP servers.

CVE-2020-15047 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.9 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
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
423453 – Trojita might not validate TLS certificates in SMTP.	Issue Tracking, Patch, Third Party Advisory, bugs.kde.org, text/html	MISC bugs.kde.org/show_bug.cgi?id=423453

Gerrit Code Review	Patch Third Party Advisory gerrit.vesnicky.cesnet.cz text/html	MISC gerrit.vesnicky.cesnet.cz/r/1035

Related QID Numbers

282325 Fedora Security Update for trojita (FEDORA-2022-46fefaadfd)

282326 Fedora Security Update for trojita (FEDORA-2022-7f67e9e695)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trojita Project	Trojita	All	All	All	All
Application	Trojita Project	Trojita	All	All	All	All

cpe:2.3:a:trojita_project:trojita:*:*:*:*:*:*:*:*:

cpe:2.3:a:trojita_project:trojita:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→