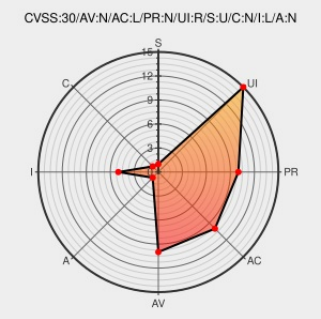
CVE-2019-10734

Published on: 04/07/2019 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2019-10734

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



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

In KDE Trojita 0.7, an attacker in possession of S/MIME or PGP encrypted emails can wrap them as sub-parts within a crafted multipart email. The encrypted part(s) can further be hidden using HTML/CSS or ASCII newline characters. This modified multipart email can be re-sent by the attacker to the intended receiver. If the receiver replies to this (benign looking) email, they unknowingly leak the plaintext of the encrypted message part(s) back to the attacker.

CVE-2019-10734 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.3 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
404697 - CVE-2019-10734: Decryption Oracle based on replying to PGP or	Exploit	MISC

404697 – CVE-2019-10734: Decryption Oracle based on replying to PGP or S/MIME encrypted emails	Exploit Third Party Advisory bugs.kde.org text/html	MISC bugs.kde.org/show_bug.cgi?id=404697

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	0.7	All	All	All
Application	Trojita Project	Trojita	0.7	All	All	All

cpe:2.3:a:trojita_project:trojita:0.7:*:*:*:*:*:*:*:

cpe:2.3:a:trojita_project:trojita:0.7:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→