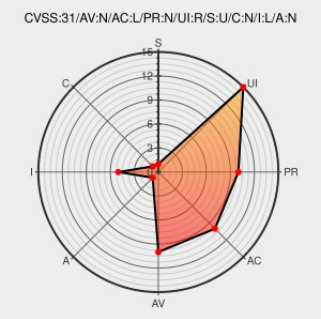
CVE-2019-10740

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

Last Modified on: 05/03/2022 02:49:00 PM UTC

CVE-2019-10740

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



Certain versions of Fedora from Fedoraproject contain the following vulnerability:

In Roundcube Webmail before 1.3.10, 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-2019-10740 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
Decryption Oracle based on replying to PGP encrypted	Exploit	MISC

Decryption Oracle based on replying to PGP encrypted emails · Issue #6638 · roundcube/roundcubemail · GitHub	Exploit Issue Tracking Third Party Advisory github.com text/html	MISC github.com/roundcube/roundcubemail/issues/6638
[security-announce] openSUSE-SU-2020:1516-1: moderate: Security update f	lists.opensuse.org text/html	SUSE openSUSE-SU-2020:1516
Release Roundcube Webmail 1.3.10 · roundcube/roundcubemail · GitHub	github.com text/html	CONFIRM github.com/roundcube/roundcubemail/releases/tag/1.3.10
[SECURITY] Fedora 29 Update: roundcubemail-1.3.10-1.fc29 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2019-d9c2f1ec70

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	29	All	All	All
Application	Opensuse	Backports Sle	15.0	sp1	All	All
Application	Opensuse	Backports Sle	15.0	sp2	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Application	Roundcube	Webmail	All	All	All	All
Application	Roundcube	Webmail	1.3.4	All	All	All
Application	Roundcube	Webmail	1.3.4	All	All	All

cpe:2.3:o:fedoraproject:fedora:29:*:*:*:*:*:*:*:

cpe:2.3:a:opensuse:backports_sle:15.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:opensuse:backports_sle:15.0:sp2:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:15.2:*:*:*:*:*:*:*:

cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*:*:*:

cpe:2.3:a:roundcube:webmail:1.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:roundcube:webmail:1.3.4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→