aDvens

Security for the greater good

Newscast

Critical vulnerability in Roundcube

2024-02-13 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

CVE-2023-43770

On 18 September 2023, Roundcube published a security advisory concerning a vulnerability in their product *Roundcube Webmail*.

This flaw, discovered by security researcher Niraj Shivtarkar, is due to improper *linkrefs* processing in the file *program/lib/Roundcube/rcube_string_replacer.php*. It allows a remote, unauthenticated attacker to inject indirect code (XSS) interpreted by the mail server.

CISA added this vulnerability to its *Known Exploited Vulnerabilities (KEV)* database on 12 February 2024.

Type of vulnerability

- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Risk

- Indirect code injection (XSS)

Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Changed
Attack complexity	Low	Impact on confidentiality	Low
Privileges Required	None	Impact on integrity	Low
User Interaction	Required	Impact on availability	None

Impacted Products

- Roundcube Webmail versions 1.4.0 tp 1.4.13
- Roundcube Webmail versions 1.5.0 to 1.5.3
- Roundcube Webmail versions 1.6.0 to 1.6.2

Recommendations

- Update Roundcube Webmail to version 1.4.14, 1.5.4, 1.6.3 or later.
- Additional information is available on the Roundcube's security advisory.

Proof of concept

A proof of concept is available in open source.

Sources

- https://www.cve.org/CVERecord?id=CVE-2023-43770
- https://roundcube.net/news/2023/09/18/security-update-1.4.14-released
- https://roundcube.net/news/2023/09/18/security-update-1.5.4-released
- https://roundcube.net/news/2023/09/15/security-update-1.6.3-released
- https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0786/
- https://www.cisa.gov/news-events/alerts/2024/02/12/cisa-adds-one-known-exploited-vulnerability-catalog