Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Roundcube Webmail Faces Unrelenting Exploitation

Date of Publication	Admiralty Code	TA Number
February 23, 2023	A1	TA2024073

Summary

First Seen: September 15, 2023
Affected Product: Roundcube Webmail
Impact: The Roundcube email server vulnerability, identified as CVE-2023-43770 and previously mitigated in September 2023, is currently being actively exploited. This flaw enables attackers to gain access to restricted information, with potential repercussions including sensitive data theft, user redirection, and unauthorized account access.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-43770	Roundcube Webmail Persistent Cross-Site Scripting (XSS) Vulnerability	Roundcube Webmail	✗	✓	✓

Vulnerability Details

#1

The vulnerability in the Roundcube email server, previously addressed in September 2023, is currently being actively exploited in attacks. This flaw, identified as CVE-2023-43770 is persistent cross-site scripting (XSS), and allows attackers to gain access to restricted information through plain text messages and maliciously crafted links. While these attacks are relatively simple in execution, they require user interaction. The potential consequences of this vulnerability are severe and diverse, including the theft of sensitive data, user redirection, and unauthorized account access.

#2

This vulnerability impacts Roundcube email servers running versions newer than 1.4.14, 1.5.x before 1.5.4, and 1.6.x before 1.6.3. With over 147,000 Roundcube servers accessible online, there is a substantial number of systems vulnerable to exploitation. These servers, easily accessible to anyone, pose a significant security risk in the absence of appropriate safeguards and defensive measures.

#3

Notably, a previous Roundcube flaw, the stored cross-site scripting vulnerability identified as CVE-2023-5631, was weaponized by threat actors with ties to Russia. The Winter Vivern Russian hacking group targeted this vulnerability as a zero-day as early as October 11, 2023. Winter Vivern operatives also exploited the CVE-2020-35730 Roundcube XSS vulnerability between August and September 2023.

#4

Similarly, the APT28 cyber-espionage group used the same bug to compromise Roundcube email servers belonging to the Ukrainian government. These types of vulnerabilities serve as common avenues for malicious cyber actors and pose substantial risks.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-43770	Roundcube before 1.4.14, 1.5.x before 1.5.4, and 1.6.x before 1.6.3	cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*:*:*	CWE-79

Recommendations

Apply Official Fixes Immediately: Apply the latest patches and updates for the Roundcube email server to address the identified vulnerability (CVE-2023-43770).

Logging and Monitoring: Enable comprehensive logging of server activities, including user interactions and system events. Regularly monitor logs for any suspicious patterns or activities that may indicate a security incident.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0042 Resource Development	TA0007 Discovery	TA0003 Persistence
T1059 Command and Scripting Interpreter	T1587.004 Exploits	T1204 User Execution	T1204.001 Malicious Link
T1082 System Information Discovery			

Patch Details

The release of Roundcube Webmail version 1.6 incorporates patches designed to address the identified issue.

Link:
https://roundcube.net/news/2023/09/15/security-update-1.6.3-released

References

https://www.cisa.gov/news-events/alerts/2024/02/12/cisa-adds-one-known-exploited-vulnerability-catalog

https://github.com/s3cb0y/CVE-2023-43770-POC

https://ethicalhacking.uk/cve-2023-43770-diving-deep-into-a-roundcube-xss-vulnerability/#gsc.tab=0

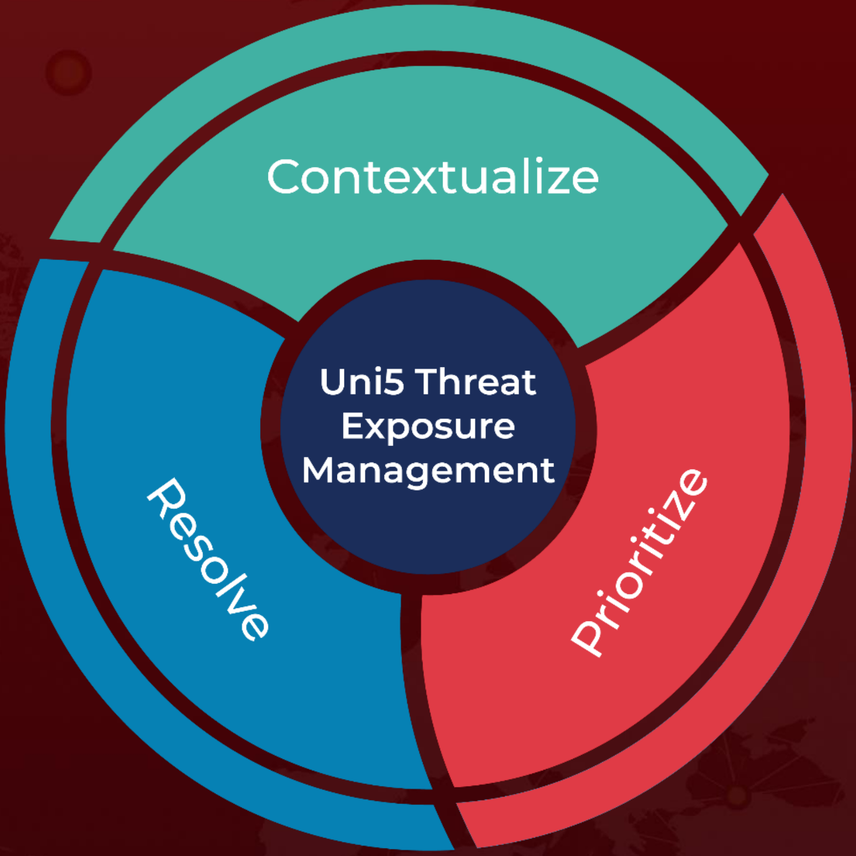
https://www.hivepro.com/threat-advisory/winter-vivern-capitalizes-on-zero-day-flaw-in-roundcube/

https://www.hivepro.com/threat-advisory/apt28-leveraged-three-roundcube-exploits-in-espionage-campaign/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 23, 2024 • 4:00 AM

More at www.hivepro.com