Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Roundcube Under Siege: Critical XSS Vulnerability Exploited in Phishing Attack

Date of Publication	Admiralty Code	TA Number
October 23, 2024	A1	TA2024406

Summary

First Seen: May 2024
Affected Products: Roundcube Webmail
Affected Industry: Government
Impact: Attackers have exploited a Cross-Site Scripting (XSS) vulnerability in the Roundcube Webmail client, designated CVE-2024-37383, in targeted phishing campaign against a governmental organization in a Commonwealth of Independent States (CIS) country. This vulnerability was leveraged to craft a sophisticated attack aimed at stealing user credentials.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-37383	Roundcube Webmail Cross-site Scripting (XSS) Vulnerability	Roundcube Webmail	✗	✓	✓

Vulnerability Details

#1

In recent months, threat actors have been observed exploiting a critical security flaw, CVE-2024-37383, in the open-source Roundcube webmail software as part of a sophisticated phishing campaign aimed at stealing user credentials. One notable attack in June 2024 targeted a governmental organization in the CIS region. The malicious email, which went undetected for months, contained a document with hidden, malicious JavaScript code that exploited the CVE-2024-37383 vulnerability, attempting to hijack the system without even displaying the attachment in the email client.

#2 This vulnerability allows attackers to execute arbitrary JavaScript on a user's webmail interface. The flaw lies in the way Roundcube processes SVG elements within the email body. Roundcube is supposed to strip out certain attributes, like "href," from SVG elements to prevent malicious code execution. However, the vulnerable function didn't account for spaces in the tag attribute, allowing threat actors to insert malicious JavaScript code that bypassed security filters.

#3 In this particular case, attackers inserted JavaScript that saved a decoy document and launched an attack aimed at harvesting login credentials using the ManageSieve plugin. The malicious HTML page was designed to prompt the victim to unknowingly enter their credentials, which were then transmitted to a server hosted on Cloudflare infrastructure, libcdn.org.

#4 Roundcube Webmail, though less widely used than some alternatives, remains a frequent target due to its adoption by government organizations and other sensitive entities. This incident underscores the importance of promptly applying patches, especially when dealing with software that handles external, untrusted environments. Roundcube users should ensure they have updated to the latest versions to mitigate the risks associated with this vulnerability and prevent potential data breaches.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-37383	Roundcube Webmail versions before 1.5.7 and Roundcube Webmail versions before 1.6.7	cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*:*	CWE-79

Recommendations

Update: Roundcube users are strongly urged to update to the latest versions 1.5.7 and 1.6.7 to address the CVE-2024-37383 vulnerability. Applying these patches is critical to mitigating the risk of exploitation and preventing potential data breaches.

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Implement Web Application Firewall (WAF): Deploy a WAF to monitor and filter incoming web traffic. A properly configured WAF can detect and block attempts to exploit the vulnerabilities, providing an additional layer of protection.

Monitor for Suspicious Activity: Regularly review logs for any unusual access patterns, particularly around the Roundcube instance, and use intrusion detection systems (IDS) to detect malicious activities.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0006** Credential Access
TA0009 Collection	**TA0011** Command and Control	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities
T1566 Phishing	**T1566.001** Spearphishing Attachment	**T1059** Command and Scripting Interpreter	**T1059.007** JavaScript
T1114 Email Collection	**T1114.002** Remote Email Collection	**T1056** Input Capture	**T1056.003** Web Portal Capture
T1204 User Execution	**T1204.002** Malicious File	**T1132** Data Encoding	**T1132.001** Standard Encoding
T1203 Exploitation for Client Execution			

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	libcdn[.]org, rcm[.]codes

Patch Details

Patches have been released to address the XSS vulnerability (CVE-2024-37383) in the Roundcube Webmail client. Users are strongly advised to update to the latest patched versions to protect their systems from potential exploitation.

Roundcube Webmail version: 1.5.7
Roundcube Webmail version: 1.6.7

Links: https://github.com/roundcube/roundcubemail/releases/tag/1.5.7

https://github.com/roundcube/roundcubemail/releases/tag/1.6.7

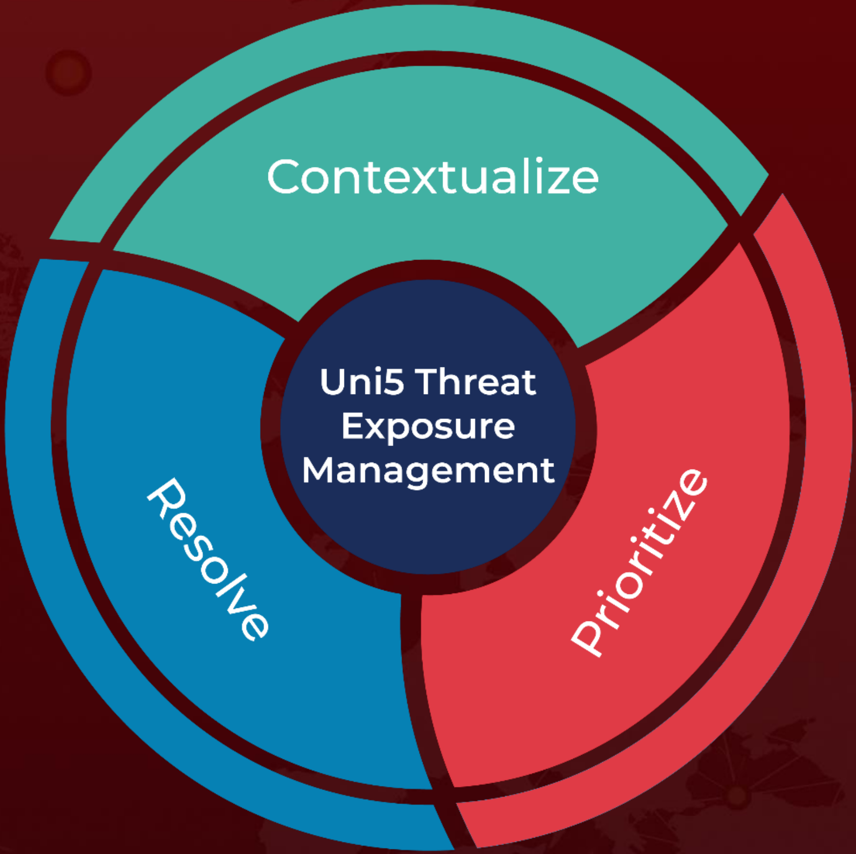
References

https://global.ptsecurity.com/analytics/pt-esc-threat-intelligence/fake-attachment-roundcube-mail-server-attacks-exploit-cve-2024-37383-vulnerability

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

October 23, 2024 • 5:20 PM

More at www.hivepro.com