Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

A Decade-Old Roundcube Glitch Comes Back to Bite

Date of Publication	Admiralty Code	TA Number
June 6, 2025	A1	TA2025177

Summary

First Seen: June 2025
Affected Products: Roundcube Webmail
Impact: A critical flaw in Roundcube Webmail (CVE-2025-49113) could let logged-in attackers run harmful code on your server. The issue, caused by poor input checks, affects millions of systems using older versions. Hackers are already sharing working exploits online, making it crucial to patch now.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-49113	Roundcube Webmail Remote Code Execution Vulnerability	Roundcube Webmail	✗	✗	✓

Vulnerability Details

#1 A newly disclosed critical vulnerability, tracked as CVE-2025-49113, has been discovered in the widely used Roundcube Webmail platform, putting millions of deployments at potential risk. This flaw, which went unnoticed for nearly a decade, allows authenticated users to execute arbitrary code remotely, effectively compromising the underlying server.

#2 The issue stems from the lack of input validation for the _from parameter in URLs processed by the upload.php script. Specifically, versions of Roundcube prior to 1.5.10 and 1.6.x before 1.6.11 are affected. Attackers can exploit this by injecting malicious payloads via PHP Object Deserialization, enabling them to gain unauthorized control over the system.

#3 The core of the vulnerability lies in the unsafe handling of the $_GET['_from'] variable, which the system deserializes without proper sanitization. This oversight can be weaponized to run harmful PHP code on the server.

#4 Shortly after a patch was released, threat actors examined the update, crafted a working exploit, and shared it on underground forums raising the urgency for defenders to respond quickly. Historically, **APT28** has exploited similar flaws in Roundcube to access sensitive emails, making this discovery particularly concerning.

#5 Organizations using Roundcube are strongly advised to upgrade to the latest fixed versions immediately, after testing the updates in their environments. Delaying the patch could leave critical infrastructure vulnerable to exploitation.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-49113	Roundcube Webmail Versions before 1.5.10 and 1.6.x before 1.6.11	cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*:*:*	CWE-502

Recommendations

Update Roundcube Without Delay: The most important step is to install the latest security patch. Make sure you're running Roundcube 1.5.10 or 1.6.11 and above, as these versions fix the vulnerability. Delaying this update could leave your server open to attacks already circulating online.

Review Server Logs for Suspicious Behavior: Look for any odd activity in your web server or Roundcube logs, especially any requests involving the upload.php file or strange _from parameter values. These might hint at attempted exploitation.

Restrict Access Where Possible: If you don't need users uploading content or changing settings frequently, limit those permissions. Only trusted or necessary accounts should have full access, especially for actions that involve file uploads or template settings.

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

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application	T1059 Command and Scripting Interpreter	

Patch Details

Update your Roundcube to the latest versions 1.5.10 or 1.6.11 and above to address the flaw.

Link: https://github.com/roundcube/roundcubemail/releases

References

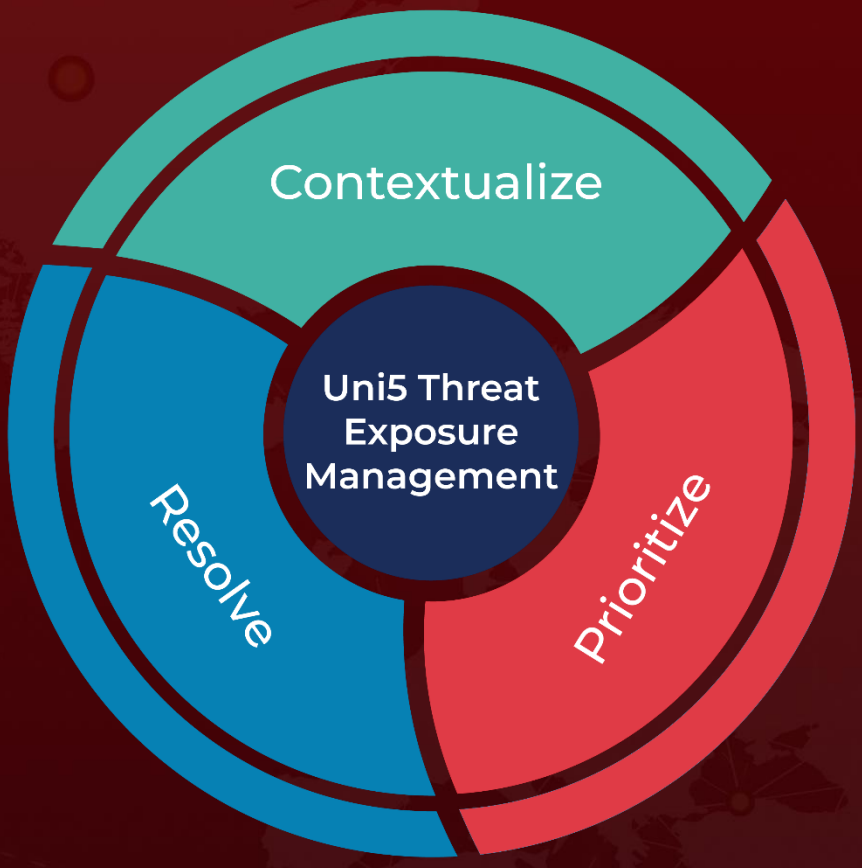
https://fearsoff.org/research/roundcube

https://hivepro.com/threat-advisory/operation-roundpress-apt28s-webmail-espionage-exposed/

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

June 6, 2025 • 6:40 AM

More at www.hivepro.com