Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

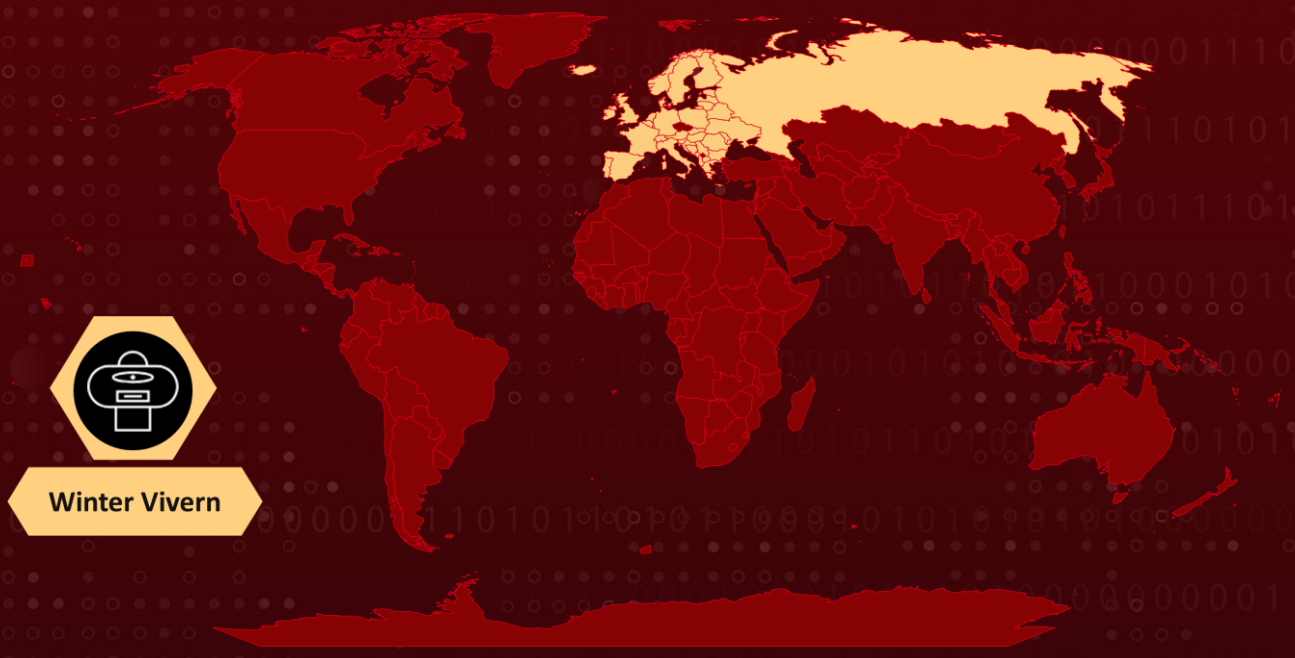
Winter Vivern Capitalizes on Zero-Day Flaw in Roundcube

Date of Publication	Admiralty Code	TA Number
October 26, 2023	A1	TA2023436

Summary

Attack Began: October 11, 2023
Attack Region: Europe
Targetted Industries: Government entities and think tank
Actor: Winter Vivern (aka UAC-0114, TA473)
Attack: The Winter Vivern cyberespionage group has been actively exploiting a zero-day vulnerability in the Roundcube webmail. The identified vulnerability, CVE-2023-5631, permits stored cross-site scripting through HTML email messages, enabling remote attackers to execute arbitrary JavaScript code. This vulnerability is leveraged by the Threat Actors to harvest email messages from the accounts of the victims.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-5631	Roundcube Cross Site Scripting Vulnerability	Roundcube	✓	✓	✓

Attack Details

#1 Winter Vivern, a cyberespionage group, has been actively exploiting a zero-day vulnerability, CVE-2023-5631, within the Roundcube webmail. They have been conducting these attacks against European government entities and their primary objective is to harvest email messages from the accounts of victims. These attacks were first detected around October 11, showcasing the group's capability to leverage previously unknown software vulnerabilities for their espionage activities..

#2 Winter Vivern group that came into public knowledge in 2021, although it is believed to have been active since at least 2020. This group focuses its attacks on governmental targets primarily located in Europe and Central Asia. To compromise their targets, Winter Vivern employs various tactics, including the distribution of malicious documents, phishing websites, and the use of a custom PowerShell backdoor. In a prior campaign, Winter Vivern was observed exploiting vulnerabilities in Roundcube, including the use of CVE-2020-35730 as recently as August and September.

#3 In recent campaign Winter Vivern group exploited the CVE-2023-5631, which is a stored cross-site scripting flaw. This vulnerability enables a remote attacker to load arbitrary JavaScript code into a target's webmail system. The attack chains typically start with a phishing mail sent containing a Base64-encoded payload embedded in the HTML source code. The payload gets decoded and injects a remote javascript, checkupdate.js, in current user session.

#4 The checkupdate.js script serves as a loader, enabling the execution of a final JavaScript payload which is designed to exfiltrate email messages. The attackers weaponized this XSS flaw to carry out their malicious activities, ultimately allowing them to harvest email messages from their victims' accounts to a C2 server. The attack chain requires minimal user interaction, the attack gets executed only in viewing the malicious email in a web browser.

#5 Winter Vivern's shift to using a zero-day vulnerability marks a notable escalation in its operations. Previously, the group relied on known vulnerabilities in Roundcube and Zimbra for which proofs of concept were available online. While Winter Vivern's toolset may not be highly sophisticated, it poses a significant threat to European governments due to its frequent phishing campaigns.

Recommendations

Apply Patch: Install the security patch provided by Roundcube to address the CVE-2023-5631 vulnerability. This patch closes the security gap that allows attackers to exploit the vulnerability.

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.

Email Security: Implement robust email filtering to counteract spam, phishing, and malicious attachments, and exercise caution with unverified links and email attachments by validating their authenticity before opening.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0007** Discovery
TA0009 Collection	**TA0011** Command and Control	**TA0010** Exfiltration	**T1583** Acquire Infrastructure
T1583.001 Domains	**T1583.004** Server	**T1587** Develop Capabilities	**T1587.004** Exploits
T1190 Exploit Public-Facing Application	**T1566** Phishing	**T1203** Exploitation for Client Execution	**T1087** Account Discovery
T1087.003 Email Account	**T1114** Email Collection	**T1114.002** Remote Email Collection	**T1071** Application Layer Protocol
T1071.001 Web Protocols	**T1041** Exfiltration Over C2 Channel		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	97ED594EF2B5755F0549C6C5758377C0B87CFAE0, 8BF7FCC70F6CE032217D9210EF30314DDD6B8135
Filename	checkupdate.js
IP	38.180.76[.]31
Domain	recsecas[.]com
Email	team.managment@outlook[.]com

Patch Link

Update your Roundcube to the latest version 1.6.4

Link: https://roundcube.net/download/

References

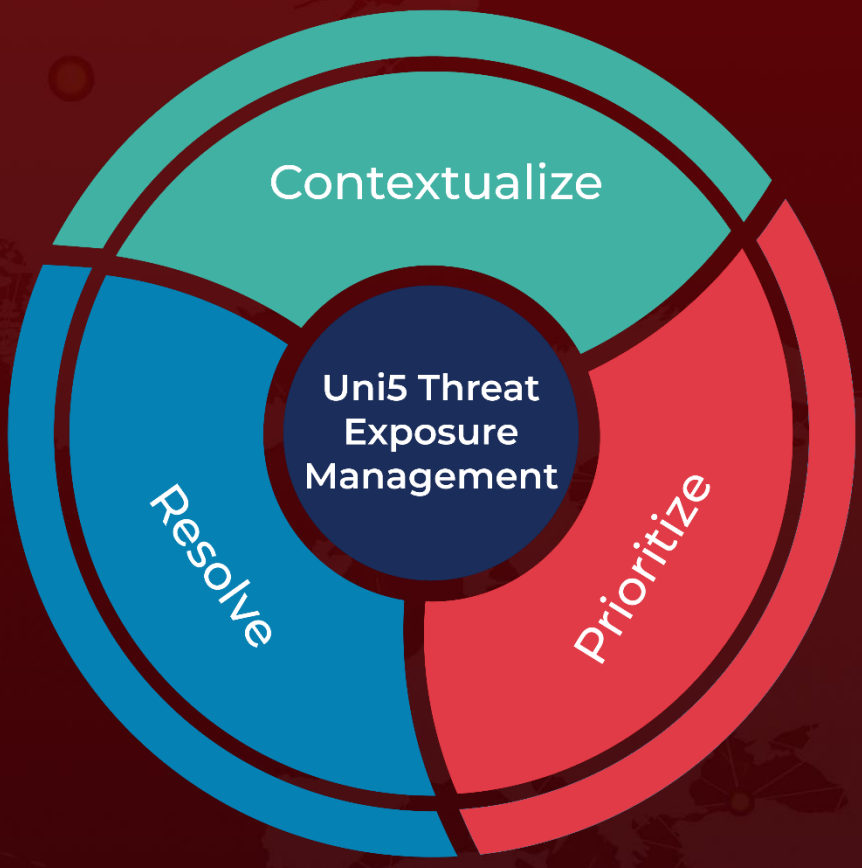
https://www.welivesecurity.com/en/eset-research/winter-vivern-exploits-zero-day-vulnerability-roundcube-webmail-servers/

https://www.hivepro.com/winter-vivern-with-pro-russian-objectives-targets-government/

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 26, 2023 . 6:10 AM

More at www.hivepro.com