

Winter Vivern exploits zero-day vulnerability in Roundcube Webmail servers

By Matthieu Faou

Archived: 2026-04-05 17:02:13 UTC

ESET Research

ESET Research recommends updating Roundcube Webmail to the latest available version as soon as possible

25 Oct 2023 • , 5 min. read



ESET Research has been closely tracking the cyberespionage operations of Winter Vivern for more than a year and, during our routine monitoring, we found that the group began exploiting a zero-day [XSS](#) vulnerability in the Roundcube Webmail server on October 11th, 2023. This is a different vulnerability than [CVE-2020-35730](#), which was also exploited by the group according to our research.

According to ESET telemetry data, the campaign targeted Roundcube Webmail servers belonging to governmental entities and a think tank, all in Europe.

Vulnerability disclosure timeline:

- **2023-10-12:** ESET Research reported the vulnerability to the Roundcube team.
- **2023-10-14:** The Roundcube team responded and acknowledged the vulnerability.
- **2023-10-14:** The Roundcube team patched the vulnerability.
- **2023-10-16:** The Roundcube team released security updates to address the vulnerability (1.6.4, 1.5.5, and 1.4.15).
- **2023-10-18:** ESET CNA issues a CVE for the vulnerability ([CVE-2023-5631](#)).
- **2023-10-25:** ESET Research blogpost published.

We would like to thank the Roundcube developers for their quick reply and for patching the vulnerability in such a short time frame.

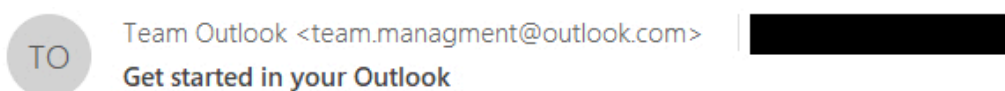
Winter Vivern profile

Winter Vivern is a cyberespionage group first revealed by [DomainTools](#) in 2021. It is thought to have been active since at least 2020 and it targets governments in Europe and Central Asia. To compromise its targets, the group uses malicious documents, phishing websites, and a custom PowerShell backdoor (see the articles from the [State Cyber Protection Centre of Ukraine](#) and from [SentinelLabs](#)). We believe with low confidence that Winter Vivern is linked to [MoustachedBouncer](#), a sophisticated Belarus-aligned group that we first published about in August, 2023.

Winter Vivern has been targeting Zimbra and Roundcube email servers belonging to governmental entities since at least 2022 – see this article from [Proofpoint](#). In particular, we observed that the group exploited [CVE-2020-35730](#), another XSS vulnerability in Roundcube, in August and September 2023. Note that [Sednit](#) (also known as APT28) is exploiting this old XSS vulnerability in Roundcube as well, sometimes against the same targets.

Technical details

Exploitation of the XSS vulnerability, assigned [CVE-2023-5631](#), can be done remotely by sending a specially crafted email message. In this Winter Vivern campaign, the emails were sent from `team.managment@outlook[.]com` and had the subject `Get started in your Outlook`, as shown in Figure 1.



Hello there!

We're the email service designed to help you conquer your day.
Connect, organize, and get things done for free across your devices.

Use Word, Excel, PowerPoint, and OneDrive for free on the web.

- Write better emails.
- Use your email and calendar together in one place.
- Personalize Outlook for your style.
- Find what you need when you need it.
- Backed by enterprise-grade security.

Register and use all the features Outlook
<https://www.microsoft.com>

Best Regards,
The Microsoft Accounts Team

This email can't receive replies. To give us feedback on this alert, [click here](#).
For more information, visit the [Microsoft Account Help Centre](#).

For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com. ESET Research offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the [ESET Threat Intelligence](#) page.

IoCs

Files

SHA-1	Filename	Detection	Description
97ED594EF2B5755F0549C6C5758377C0B87CFAE0	checkupdate.js	JS/WinterVivern.B	JavaScript loader.
8BF7FCC70F6CE032217D9210EF30314DDD6B8135	N/A	JS/Kryptik.BIK	JavaScript payload exfiltrating emails in Roundcube.

Network

IP	Domain	Hosting provider	First seen	Details
38.180.76[.]31	recsecas[.]com	M247 Europe SRL	2023-09-28	Winter Vivern C&C server

Email addresses

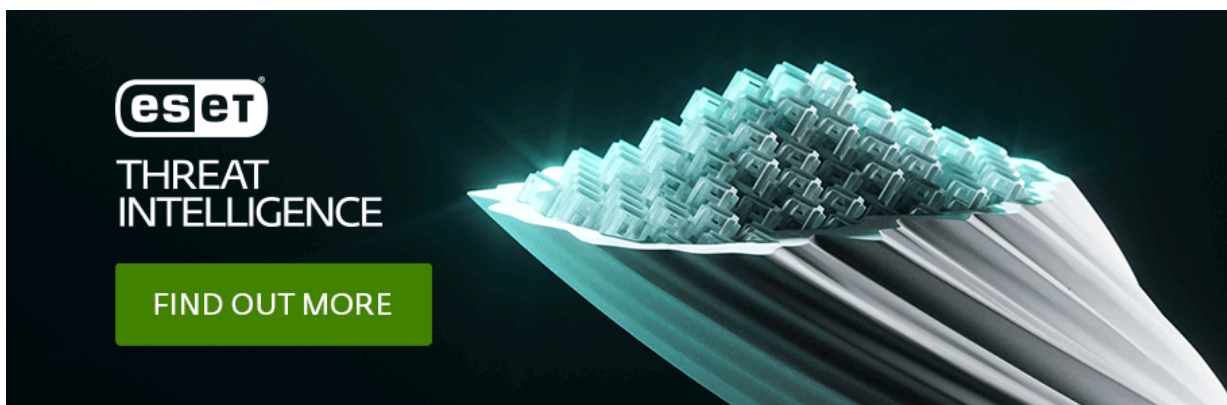
team.managment@outlook[.]com

MITRE ATT&CK techniques

This table was built using [version 13](#) of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Resource Development	T1583.001	Acquire Infrastructure: Domains	Winter Vivern operators bought a domain at Registrar.eu.
	T1583.004	Acquire Infrastructure: Server	Winter Vivern operators rented a server at M247.
	T1587.004	Develop Capabilities: Exploits	Winter Vivern operators probably developed an exploit for Roundcube.

Tactic	ID	Name	Description
Initial Access	T1190	Exploit Public-Facing Application	Winter Vivern sent an email exploiting CVE-2023-5631 in Roundcube.
	T1566	Phishing	The vulnerability is triggered via a phishing email, which should be opened in the Roundcube webmail by the victim.
Execution	T1203	Exploitation for Client Execution	The JavaScript payload is executed by an XSS vulnerability in Roundcube.
Discovery	T1087.003	Account Discovery: Email Account	The JavaScript payload can list folders in the email account.
Collection	T1114.002	Email Collection: Remote Email Collection	The JavaScript payload can exfiltrate emails from the Roundcube account.
Command and Control	T1071.001	Application Layer Protocol: Web Protocols	C&C communications use HTTPs.
Exfiltration	T1041	Exfiltration Over C2 Channel	Exfiltration is done via HTTPs and to the same C&C server.



Let us keep you up to date

Sign up for our newsletters



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