ESET Research: Winter Vivern attacks Roundcube webmail servers of governments in Europe through zero-day vulnerability

DUBAI, UNITED ARAB EMIRATES, November 1, 2023 /EINPresswire.com/ -- ESET researchers, during their regular monitoring of the cyberespionage operations of Winter Vivern, discovered that the group recently began exploiting a zero-day XSS vulnerability in the Roundcube Webmail server. In an XSS attack, malicious scripts are injected into otherwise trusted websites. According to ESET telemetry data, the campaign targeted Roundcube Webmail servers belonging to governmental entities and a think tank, all in Europe. ESET Research recommends updating Roundcube Webmail to the latest available version as soon as possible.

ESET discovered the vulnerability on October 12 and immediately reported it to the Roundcube team, who patched the vulnerability and released security updates soon after, on October 14. “We would like to thank the Roundcube developers for their quick reply and for patching the vulnerability in such a short time frame,” says ESET researcher Matthieu Faou, who discovered the vulnerability and Winter Vivern attacks.

“Winter Vivern is a threat to governments in Europe because of its persistence, its very consistent running of phishing campaigns, and because a significant number of internet-facing applications are not regularly updated despite being known to contain vulnerabilities,” explains Faou.

Exploitation of the XSS vulnerability CVE-2023-5631 can be done remotely by sending a specially crafted email message.

“At first sight, the email doesn’t seem malicious – but if we examine the HTML source code, we can see a tag for SVG graphics at the end that contains an encoded malicious payload,” says Faou. 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 final JavaScript payload can exfiltrate email messages to the command and control server of the group.

Winter Vivern is a cyberespionage group that is thought to have been active since at least 2020 and targets governments in Europe and Central Asia. To compromise its targets, the group uses malicious documents, phishing websites, and a custom PowerShell backdoor. ESET believes 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.

For more technical information about Winter Vivern, its latest attack, and the Roundcube vulnerability, check out the blogpost "Winter Vivern exploits zero-day vulnerability in Roundcube Webmail servers" on WeLiveSecurity. Make sure to follow ESET Research on Twitter (now known as X) for the latest news from ESET Research.

About ESET
For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and X (Twitter).

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here