Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

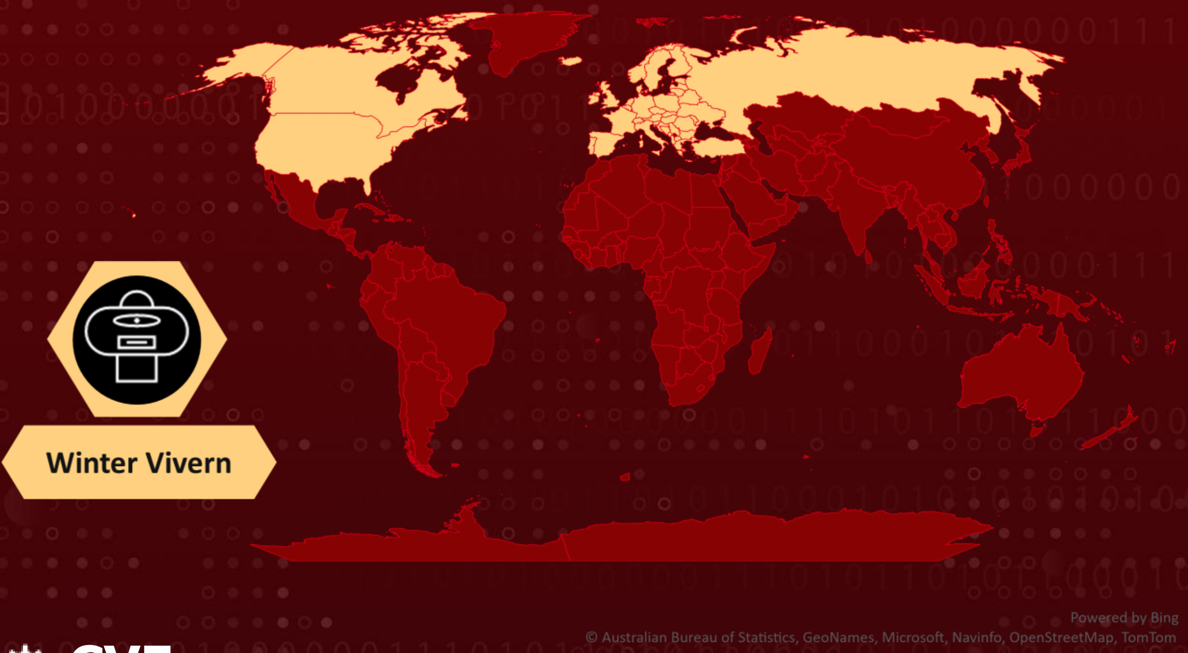
Winter Vivern APT targets EU with Zimbra flaw

Date of Publication	Admiralty Code	TA Number
April 4, 2023	A1	TA2023170

Summary

Attack began: February 2023
Actor: Winter Vivern (aka TA473 and UAC-0114)
Attack Region: Europe and NATO.
Targeted Industries: Government, Telecommunications, Private businesses, military, and diplomatic organizations
Attack: Winter Vivern abuses CVE-2022-27926 to attack public Zimbra webmail portals of government entities.

Attack Regions


Winter Vivern
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

CVEs

CVE	NAME	AFFECTED PRODUCT	CISA KEV	PATCH
CVE-2022-27926	Zimbra Collaboration (ZCS) Cross-Site Scripting (XSS) Vulnerability	Zimbra Collaboration: 9.0.0 P23	✓	✓

Attack Details

#1 Winter Vivern, also known as TA473, exploits the Zimbra vulnerability CVE-2022-27926 to gain unauthorized access to publicly accessible webmail portals. They aim to obtain sensitive emails from military, government, and diplomatic groups involved in the Russia-Ukraine conflict across Europe. The group uses scanning tools like Acunetix to locate unpatched webmail gateways of these entities and devise targeted attack strategies.

#2 The phishing emails contain a link that injects other JavaScript payloads onto the webpage by exploiting CVE-2022-27926 in the target's compromised Zimbra infrastructure. These payloads are then utilized to extract usernames, passwords, and tokens from cookies sent by the compromised Zimbra endpoint. This information enables threat actors to readily access the targets' email accounts.

Recommendations

- Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

- It is encouraged to take proactive security steps, such as blocking Indicators of Compromise (IoCs) and upgrading to Zimbra Collaboration 9.0.0 P24 is an effective way to address the Zimbra XSS vulnerability. Additionally, boosting the security posture requires the implementation of preventive and detection mechanisms, such as defining a firewall rule to restrict inbound/outbound traffic to/from the attacker's IP address.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
TA0009 Collection	T1027 Obfuscated Files or Information	T1068 Exploitation for Privilege Escalation	T1134 Access Token Manipulation
T1566 Phishing	T1555 Credentials from Password Stores	T1114 Email Collection	

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps[:]//oscp-avanguard[.]com/asn15180YHASIFHOP_<redacted>_ASNfas21/auth.js hxxps[:]//oscp-avanguard[.]com/settingPopImap/SettingupPOPandIMAPaccounts.html hxxps[:]//troadsecow[.]com/cbzc.policja.gov.pl hxxps[:]//bugiplaysec[.]com/mgu/auth.js hxxps[:]//nepalihemp[.]com/assets/img/images/623930va hxxps[:]//ocs-romastassec[.]com/redirect/?id=[target specific ID]&url=[Base64 Encoded Hyperlink URL hochuzhit-com.translate.goog/?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en-US&x_tr_pto=wapp] hxxps[:]//ocspdep[.]com/inotes.sejm.gov.pl?id=[Target Specific SHA256 Hash]
Domains	ocspdep[.]com bugiplaysec[.]com oscp-avanguard[.]com troadsecow[.]com nepalihemp[.]com

Patch Details

Update Zimbra Collaboration 9.0.0 P24

Patch Link
https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P24

References

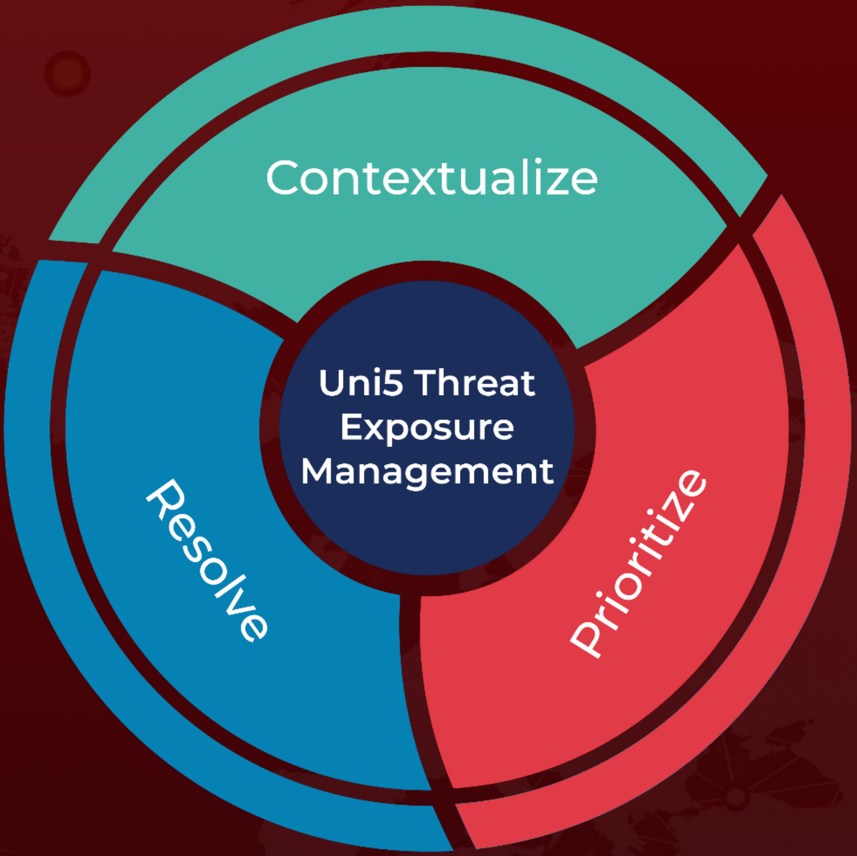
https://www.proofpoint.com/us/blog/threat-insight/exploitation-dish-best-served-cold-winter-vivern-uses-known-zimbra-vulnerability

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

April 4, 2023 • 7:56 AM

More at www.hivepro.com