Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

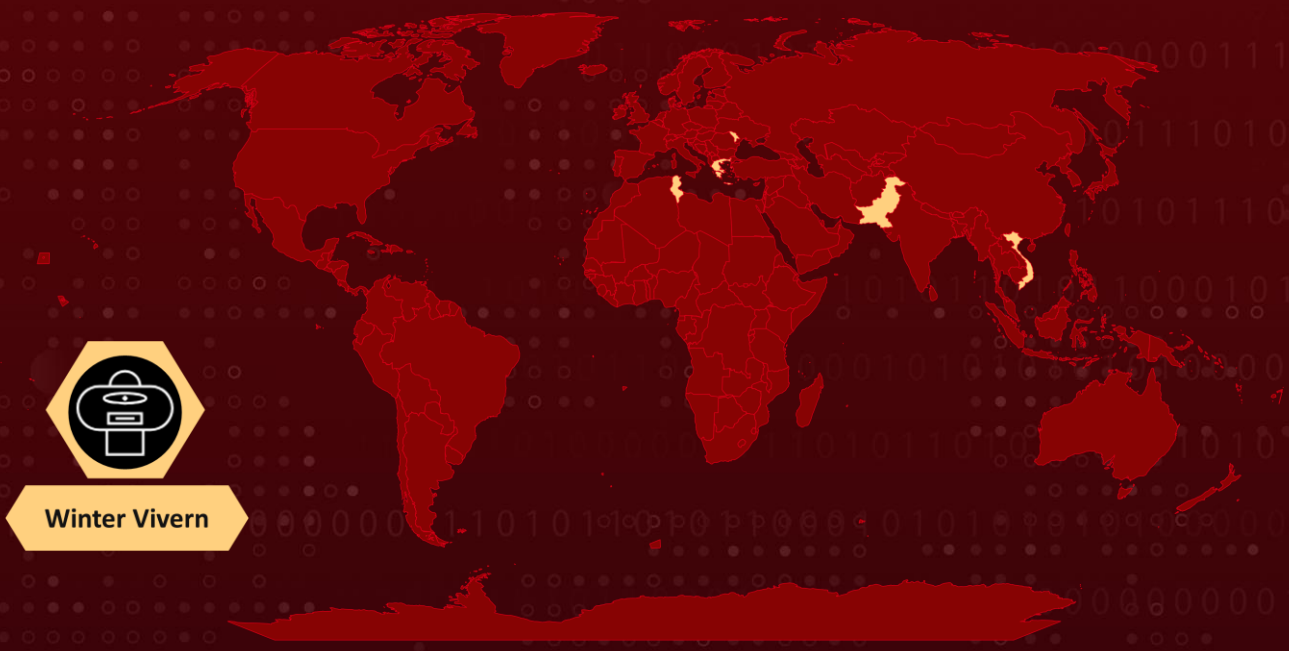
Four Threat Actors Capitalized on Zimbra Zero Day to Infiltrate Government Organizations

Date of Publication	Admiralty Code	TA Number
November 17, 2023	A1	TA2023464

Summary

Attack Discovered: June 29, 2023
Attack Region: Greece, Moldova, Tunisia, Vietnam, Pakistan
Targetted Indutries: Government Organization
Actor: Winter Vivern
Attack: A zero-day vulnerability identified as CVE-2023-37580 in Zimbra Collaboration email software has been exploited by four different groups in attacks. These attacks aimed to illicitly obtain email data, user credentials, and authentication tokens.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-37580	Zimbra Collaboration (ZCS) Cross-Site Scripting (XSS) Vulnerability	Zimbra Collaboration (ZCS)	✓	✓	✓

Attack Details

#1 A zero-day vulnerability, identified as CVE-2023-37580, in the Zimbra Collaboration email software has been exploited by four distinct groups in real-world attacks. This exploitation has been utilized by threat actors to illicitly access and steal email data, user credentials, and authentication tokens.

#2 The CVE-2023-37580, is a reflected cross-site scripting (XSS) issue resulting from insufficient sanitization of user-supplied data in the Zimbra Classic Web Client. This flaw allows a remote attacker to execute arbitrary script code in the user's browser by deceiving the victim into following a specially crafted link. The vulnerability was actively exploited in targeted attacks against Zimbra's email server in June. Hotfixes were publicly disclosed on GitHub on July 5, 2023, and the official patch was released on July 25, 2023.

#3 In the initial campaign, a government organization in Greece was the target, receiving emails with exploit URLs. Clicking these URLs resulted in the delivery of email-stealing malware. This framework utilized the XSS vulnerability to pilfer users' email data, including emails and attachments, and established an auto-forwarding rule to redirect emails to an email address controlled by the attacker.

#4 Winter Vivern, the second threat actor exploiting CVE-2023-37580, focused on government organizations in Moldova and Tunisia. Notably, these attacks occurred shortly after a hotfix for the vulnerability was made available on GitHub on July 5, before the patch was released.

#5 In the third campaign, an unidentified group exploited the vulnerability to conduct phishing attacks targeting credentials of a government organization in Vietnam. The exploit URL led to a script that presented a phishing page for users' webmail credentials. The stolen credentials were then posted to a URL hosted on an official government domain that the attackers had compromised.

#6 In the fourth campaign, a government organization in Pakistan was targeted on August 25 using the vulnerability. This resulted in the exfiltration of the Zimbra authentication token to a remote domain. It's noteworthy that this campaign occurred after the official patch had been released. The campaigns exploiting CVE-2023-37580 demonstrate the importance of timely mail server fixes and how attackers monitor open-source repositories to exploit vulnerabilities not yet released to users.

Recommendations

- **Apply the Official Patch (ZCS 8.8.15 Patch 41):** Install the provided security patch from Zimbra to address the CVE-2023-37580 XSS vulnerability in version 8.8.15. This patch effectively closes the security gap and prevents potential data compromise.
- **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.
- **Network Segmentation and Access Controls**: Restrict access to the Zimbra server through network segmentation and access controls. By isolating the server and controlling permissions, you reduce the risk of unauthorized access and limit potential damage from successful attacks.
- **Implement Web Application Firewall (WAF):** Deploy a WAF to monitor and filter incoming web traffic to the Zimbra Classic Web Client. A properly configured WAF can detect and block attempts to exploit the XSS vulnerability, providing an additional layer of protection.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion
TA0006 Credential Access	TA0010 Exfiltration	T1588 Obtain Capabilities	T1588.006 Vulnerabilities
T1588.005 Exploits	T1566 Phishing	T1059 Command and Scripting Interpreter	T1134 Access Token Manipulation
T1190 Exploit Public-Facing Application			

Indicators of Compromise (IOCs)

TYPE	VALUE
URL	hxxps://obsorth.opwtjnpoc[.]ml/pQyMSCXWyBWJpIos.js, hxxps://applicationdevsoc[.]com/zimbraMalwareDefender/zimbraDefender.js, hxxps://applicationdevsoc[.]com/tndgt/auth.js, ntcpk[.]org

Patch Details

To address the vulnerability, it is essential to upgrade versions of the Zimbra Collaboration Suite to ZCS 8.8.15 Patch 41 or later.

Link:
https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P41

https://wiki.zimbra.com/wiki/Security_Center

References

https://blog.google/threat-analysis-group/zimbra-0-day-used-to-target-international-government-organizations/

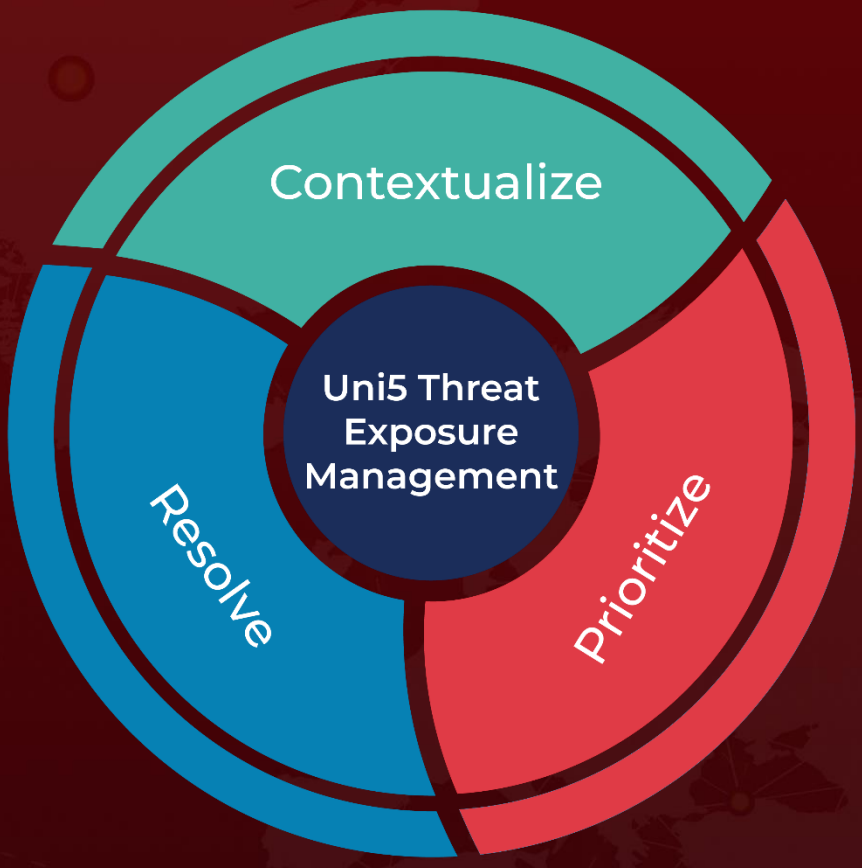
https://www.hivepro.com/threat-advisory/zimbra-fixes-a-zero-day-vulnerability-exploited-in-attacks/

https://www.hivepro.com/threat-advisory/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

November 17, 2023 . 4:00 AM

More at www.hivepro.com