Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Zimbra Fixes A Zero-Day Vulnerability Exploited in Attacks

Date of Publication	Admiralty Code	TA Number
July 28, 2023	A1	TA2023317

Summary

First Seen: July 13, 2023
Affected Platforms: Zimbra Collaboration (ZCS)
Impact: The vulnerability (CVE-2023-37580) in Zimbra Collaboration Suite (ZCS) version 8.8.15 is a Cross-Site Scripting (XSS) flaw in the Zimbra Classic Web Client interface. Its impact is severe as it can compromise the confidentiality and integrity of the user's data. The exploitation of this vulnerability has already been observed in targeted cyberattacks, posing significant risks to the affected systems and their users.

CVEs

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

Vulnerability Details

#1

Zimbra has released security update to protect users from a zero-day vulnerability (CVE-2023-37580) discovered by Clément Lecigne of Google Threat Analysis Group. This flaw affects Zimbra Collaboration Suite (ZCS) mail servers in version 8.8.15 and is a Cross-Site Scripting (XSS) issue in the Zimbra Classic Web Client interface, posing a risk to data confidentiality and integrity. XSS attacks are dangerous as they allow threat actors to steal sensitive information or execute malicious code on vulnerable systems. The vulnerability has already been exploited in targeted cyberattacks.

#2

Before the official fix, Zimbra had provided an alert with a manual solution for administrators. Now, an update is available to address the security flaw. Additionally, Zimbra has released two more security patches, including one for CVE-2023-38750, which could expose internal JSP and XML files. The update also includes an OpenSSL package upgrade to fix CVE-2023-0464.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-37580	Zimbra Collaboration: 8.8.15 - 8.8.15 Patch 40	cpe:2.3:a:synacor:zimbra_collaboration:8.8.15:Patch 40:*:*:*:*:*:*:*	CWE-79

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.

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.

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.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0040 Impact
T1189 Exploit Public-Facing Application	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1588.005 Exploits

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.

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

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

References

https://www.cisa.gov/news-events/alerts/2023/07/27/cisa-adds-one-known-exploited-vulnerability-catalog

https://blog.zimbra.com/2023/07/security-update-for-zimbra-collaboration-suite-version-8-8-15/

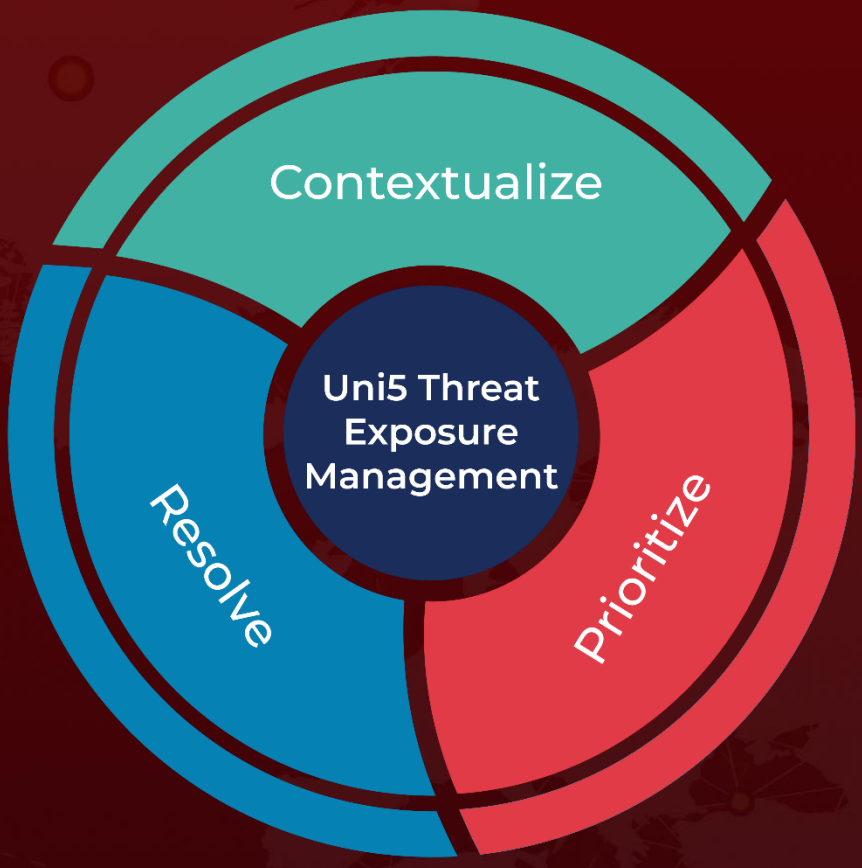
https://twitter.com/Zimbra/status/1679477778092097538

https://twitter.com/maddiestone/status/1679542322772721664

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

July 28, 2023 • 4:30 AM

More at www.hivepro.com