Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Zimbra Zero-Day Hidden in "Harmless" ICS File Targets Military

Date of Publication	Admiralty Code	TA Number
October 10, 2025	A1	TA2025310

Summary

First Seen: Early 2025
Affected Product: Synacor Zimbra Collaboration Suite (ZCS)
Targeted Country: Brazil
Targeted Industry: Military
Impact: In early 2025, an unidentified actor impersonating the Libyan Navy's Office of Protocol targeted Brazil's military with a malicious calendar file exploiting a zero-day flaw in Zimbra Collaboration Suite (CVE-2025-27915). The attack leveraged concealed JavaScript to steal data and manipulate emails, marking a rare and sophisticated exploitation of open-source collaboration software.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-27915	Synacor Zimbra Collaboration Suite (ZCS) Cross-site Scripting Vulnerability	Synacor Zimbra Collaboration Suite (ZCS)	✓	✓	✓

Vulnerability Details

#1 In early 2025, an unidentified threat actor impersonated the Libyan Navy's Office of Protocol to launch a sophisticated cyberattack against Brazil's military. The operation delivered a zero-day exploit targeting CVE-2025-27915, a cross-site scripting (XSS) vulnerability in Zimbra Collaboration Suite (ZCS) versions 9.0, 10.0, and 10.1 through a malicious calendar file (ICS).

#2 This method was unusual, marking one of the few recorded cases in which attackers exploited open-source collaboration software like Zimbra through email attachments rather than the more common tactics of phishing or direct server compromise.

#3

ICS, or iCalendar files, are plain-text formats used to store and share scheduling data across different calendar platforms. In this campaign, the attackers weaponized such a file by embedding malicious JavaScript code that executed when a target viewed the calendar entry. The exploit leveraged an ontoggle event within a <details> tag, enabling arbitrary code execution inside the victim's browser session.

#4

Once triggered, the payload granted attackers the ability to manipulate email settings, redirect communications, and exfiltrate sensitive data. The vulnerability itself stemmed from insufficient sanitization of HTML content in ICS calendar files handled by Zimbra's Classic Web Client. This flaw enabled stored XSS attacks, which could lead to remote code execution.

#5

The malicious code was designed as an information stealer, capable of harvesting user credentials, emails, contacts, and shared folders. Stolen information was transmitted to attacker-controlled servers. To avoid detection, the attackers employed several obfuscation measures, including a 60-second delay before execution and restricting re-execution to once every three days.

#6

The malicious ICS file actively monitored user behavior, exfiltrated data in real time, and automatically logged users out after inactivity to capture fresh credentials upon their next login. Although the exact perpetrators remain unidentified, similar operations in the past have been linked to Russian threat groups that exploited XSS vulnerabilities. Groups like UNC1151 (Ghostwriter) have employed comparable methods to conduct credential theft campaigns.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-27915	Zimbra Collaboration (ZCS) 9.0, 10.0, and 10.1	cpe:2.3:a:zimbra:collaboration:*:*:*:*:*:*:*:*	CWE-79

Recommendations

Security Patching and Vulnerability Mitigation: Immediate patching is required to address CVE-2025-27915. Install Zimbra 9.0.0 P44, 10.0.13, or 10.1.5, all of which contain the necessary security fixes. Until patching is complete, the Classic Web Client should be disabled to reduce exposure. Organizations should temporarily strip or quarantine ICS files at the mail gateway to prevent exploitation.

End-of-Life (EOL) for Zimbra Collaboration Suite: ZCS 9.0 reached End of Life on June 30, 2025, and ZCS 10.0 reached End of General Support on the same date. No security updates, patches, or feature enhancements are provided for these versions. Organizations still using them must migrate immediately to ZCS 10.1 and the currently supported version, to ensure continued protection and access to the latest functionality.

Operating System Deprecation Considerations: Support for Zimbra on RHEL/CentOS 7 and Oracle 7 was deprecated following the release of Zimbra 10.1.10 in July 2025. Both RHEL/CentOS 7 and Oracle 7 had already reached their OS-level EOL, leaving installations on these platforms vulnerable. Customers were strongly advised to migrate to RHEL, Rocky, or Oracle Linux 9 for all future installations to maintain security compliance and ensure continued support.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0009** Collection	**TA0010** Exfiltration	**TA0011** Command and Control
T1190 Exploit Public-Facing Application	**T1203** Exploitation for Client Execution	**T1059** Command and Scripting Interpreter	**T1114** Email Collection
T1059.007 JavaScript	**T1098** Account Manipulation	**T1098.002** Additional Email Delegate Permissions	**T1078** Valid Accounts

T1027 Obfuscated Files or Information	T1036 Masquerading	T1564 Hide Artifacts	T1656 Impersonation
T1041 Exfiltration Over C2 Channel	T1071.001 Web Protocols	T1071 Application Layer Protocol	T1056 Input Capture

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	193[.]29[.]58[.]37
URL	hxxps[:]//ffrk[.]net/apache2_config_default_51_2_1
Email	spam_to_junk[@]proton[.]me
SHA256	ea752b1651ad16bc6bf058c34d6ae795d0b4068c2f48fdd7858f3d4f7c516f37

Patch Details

Apply the patch immediately. Zimbra versions 9.0.0 P44, 10.0.13, and 10.1.5 include security fixes addressing CVE-2025-27915.

Links:
https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.13

https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.5

https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P44

References

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

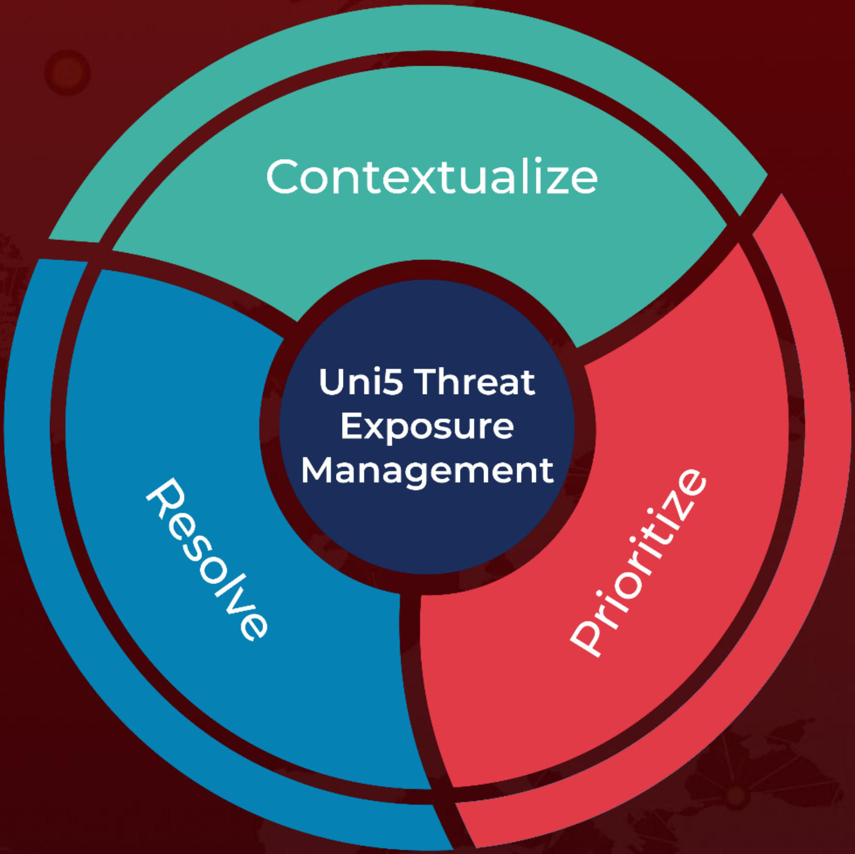
https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.9

https://strikeready.com/blog/0day-ics-attack-in-the-wild/

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

October 10, 2025 • 02:00 AM

More at www.hivepro.com