THREAT BULLETINS

Threat Actors Exploiting Multiple Vulnerabilities Against Zimbra Collaboration Suite

TLP:WHITE

Aug 16, 2022

On August 16, 2022, the Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information and Analysis Center (MS-ISAC) released a Joint Cybersecurity Advisory (AA22-228A) in response to **active exploitation** of multiple Common Vulnerabilities and Exposures (CVEs) against the enterprise cloud-hosted collaboration software and email platform, **Zimbra Collaboration Suite (ZCS)**.

The CVEs currently being exploited against Zimbra Collaboration Suite include:

- CVE-2022-24682
- CVE-2022-27924
- CVE-2022-27925 chained with CVE-2022-37042
- CVE-2022-30333

Cyber threat actors are potentially targeting unpatched Zimbra Collaboration Suite instances in both government and private sector networks. CISA and the MS-ISAC

strongly urge users and administrators to apply the guidance provided in the **Recommendations** section of the alert to help secure their organization's systems against malicious cyber activity. CISA and the MS-ISAC encourage organizations to assume compromise and hunt for malicious activity using the third-party detection signatures in the **Detection Methods** section if their ZCS instances were not immediately updated upon patch release, or the instances were exposed to the internet. Additionally, organizations that detect potential compromise should apply the steps in the **Incident Response** section of the alert.

All members are encouraged to review AA22-228A: Threat Actors Exploiting Multiple CVEs Against Zimbra Collaboration Suite for the technical details provided, detection methods, and incident response recommendations.

CVE-2022-27924

CVE-2022-27924 is a high-severity vulnerability enabling an unauthenticated malicious actor to inject arbitrary memcache commands into a targeted ZCS instance and cause an overwrite of arbitrary cached entries. The actor can then steal ZCS email account credentials in cleartext form without any user interaction. With valid email account credentials in an organization not enforcing multifactor authentication (MFA), a malicious actor can use spear phishing, social engineering, and business email compromise (BEC) attacks against the compromised organization. Additionally, malicious actors could use the valid account credentials to open webshells and maintain persistent access.

On March 11, 2022, researchers from SonarSource announced the discovery of this ZCS vulnerability. Zimbra issued fixes for releases 8.8.15 and 9.0 on May 10, 2022. In June 2022, SonarSource publicly released proof-of-concept (POC) exploits for this vulnerability. Based on evidence of active exploitation, CISA added this vulnerability to the Known Exploited Vulnerabilities Catalog on August 4, 2022. Due to the POC and ease of exploitation, CISA and the MS-ISAC expect to see widespread exploitation of unpatched ZCS instances in government and private networks.

CVE-2022-27925 and CVE-2022-73042

CVE-2022-27925 is a high severity vulnerability in ZCS releases 8.8.15 and 9.0 that have mboximport functionality to receive a ZIP archive and extract files from it. An authenticated user has the ability to upload arbitrary files to the system thereby leading to directory traversal. On August 10, 2022, researchers from Volexity reported widespread exploitation—against over 1,000 ZCS instances—of CVE-2022-27925 in conjunction with CVE-2022-37042. CISA added both CVEs to the Known Exploited Vulnerabilities Catalog on August 11, 2022.

CVE-2022-37042 is an authentication bypass vulnerability that affects ZCS releases 8.8.15 and 9.0. CVE-2022-37042 could allow an unauthenticated malicious actor access to a vulnerable ZCS instance. According to Zimbra, CVE-2022-37042 is found in the MailboxImportServlet function. Zimbra issued fixes in late July 2022.

CVE-2022-30333

CVE-2022-30333 is a high-severity directory traversal vulnerability in RARLAB UnRAR on Linux and UNIX allowing a malicious actor to write to files during an extract (unpack) operation. A malicious actor can exploit CVE-2022-30333 against a ZCS server by sending an email with a malicious RAR file. Upon email receipt, the ZCS server would automatically extract the RAR file to check for spam or malware. Any ZCS instance with unrar installed is vulnerable to CVE-2022-30333.

Researchers from SonarSource shared details about this vulnerability in June 2022. Zimbra made configuration changes to use the 7zip program instead of unrar. CISA added CVE-2022-3033 to the Known Exploited Vulnerabilities Catalog on August 9, 2022. Based on industry reporting, a malicious cyber actor is selling a cross-site scripting (XSS) exploit kit for the ZCS vulnerability to CVE 2022 30333. A Metasploit module is also available that creates a RAR file that can be emailed to a ZCS server to exploit CVE-2022-30333.

CVE-2022-24682

CVE-2022-24682 is a medium-severity vulnerability that impacts ZCS webmail clients running releases before 8.8.15 patch 30 (update 1), which contains a cross-site scripting (XSS) vulnerability allowing malicious actors to steal session cookie files. Researchers from Volexity shared this vulnerability on February 3, 2022, and Zimbra issued a fix on February 4, 2022. CISA added this vulnerability to the Known Exploited Vulnerabilities Catalog on February 25, 2022.

Detection Methods:

CISA recommends administrators, especially at organizations that did not immediately update their ZCS instances upon patch release, to hunt for malicious activity using the following third-party detection signatures:

- Hunt for IOCs including:
  - 207.148.76[.]235 – a Cobalt Strike command and control (C2) domain
- Deploy third-party YARA rules to detect malicious activity, here

Mitigations

CISA and the MS-ISAC recommend organizations upgrade to the latest ZCS releases as noted on Zimbra Security – News & Alerts and Zimbra Security Advisories.

See Volexity's Mass Exploitation of (Un)authenticated Zimbra RCE: CVE-2022-27925 for mitigation steps.

Additionally, CISA and the MS-ISAC recommend organizations apply the following best practices to reduce the risk of compromise:

- Maintain and test an incident response plan.
- Ensure your organization has a vulnerability management program in place and that it prioritizes patch management and vulnerability scanning of known exploited vulnerabilities. Note: CISA's Cyber Hygiene Services (CyHy) are free to all state, local, tribal, and territorial (SLTT) organizations, as well as public and private sector critical infrastructure organizations: cisa.gov/cyber-hygiene-services.
- Properly configure and secure internet-facing network devices.
  - Do not expose management interfaces to the internet.
  - Disable unused or unnecessary network ports and protocols.
  - Disable/remove unused network services and devices.
- Adopt zero-trust principles and architecture, including:
  - Micro-segmenting networks and functions to limit or block lateral movements.
  - Enforcing phishing-resistant multifactor authentication (MFA) for all users and VPN connections.
  - Restricting access to trusted devices and users on the networks.

Incident Response:

If an organization's system has been compromised by active or recently active threat actors in their environment, CISA and the MS-ISAC recommend the following initial steps:

1. Collect and review artifacts, such as running processes/services, unusual authentications, and recent network connections.
2. Quarantine or take offline potentially affected hosts.
3. Re-image compromised hosts.
4. Provision new account credentials.
5. Report the compromise to CISA via CISA's 24/7 Operations Center (report@cisa.gov or 888-282-0870). SLTT government entities can also report to the MS-ISAC (SOC@cisecurity.org or 866-787-4722).

See the Joint CSA from the cybersecurity authorities of Australia, Canada, New Zealand, the United Kingdom, and the United States on Technical Approaches to Uncovering and Remediating Malicious Activity for additional guidance on hunting or investigating a network, and for common mistakes in incident handling. CISA and the MS-ISAC also encourage government network administrators to see CISA's Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. Although tailored to federal civilian branch agencies, these playbooks provide operational procedures for planning and conducting cybersecurity incident and vulnerability response activities and detail steps for both incident and vulnerability response.

Reference(s)	CISA, Volexity, GitHub

Recommendations
AA22-228A: Threat Actors Exploiting Multiple CVEs Against Zimbra Collaboration Suite

Volexity: Mass Exploitation of (Un)authenticated Zimbra RCE: CVE-2022-27925

YARA Rules

Alert ID e29c6b14

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

Tags Joint CSA, Zimbra Collaboration Suite (ZCS)

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.