THREAT BULLETINS

Update - Threat Actors Exploiting Multiple Vulnerabilities Against Zimbra Collaboration Suite

TLP:WHITE

Sep 28, 2022

The following document is an updated version of the previously shared alert AA22-228A, distributed by Health-ISAC. The previously distributed alert is available for review here. The major updates shared are the Malware Analysis Reports linked below under the heading *Update September 27, 2022.*

The Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing & Analysis Center (MS-ISAC) are publishing this joint Cybersecurity Advisory (CSA) in response to active exploitation of multiple Common Vulnerabilities and Exposures (CVEs) against Zimbra Collaboration Suite (ZCS), an enterprise cloud-hosted collaboration software and email platform. CVEs currently being exploited against ZCS include:

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

Cyber threat actors may be targeting unpatched ZCS instances in both government and private sector networks. CISA and the MS-ISAC strongly urge users and administrators to apply the guidance in the Recommendations section to help secure their organization's systems against malicious cyber activity.

Organizations who did not immediately update their ZCS instances upon patch release, or whose ZCS instances were exposed to the internet, are encouraged to assume compromise and hunt for malicious activity using the third-party detection signatures in the Detection Methods section of the CSA. Organizations that detect potential compromise should apply the steps provided in the Incident Response section.

Update September 27, 2022:

The CSA has been updated with additional IOCs which have been provided by the following Malware Analysis Reports (MARs) below:

- MAR-10400779-1
- MAR-10400779-2
- MAR-10401765-1

Technical Details:

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. Based on evidence of active exploitation, CISA added this vulnerability to the Known Exploited Vulnerabilities Catalog on August 4, 2022. Due to 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-2022-37042

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.[6] 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 contain 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:

Note: CISA and the MS-ISAC will update this section with additional IOCs and signatures as further information becomes available.

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:

- ***Update September 27, 2022***: Hunt for IOCs including:

IP Addresses	Note
62.113.255[.]70	**New September 27, 2022:** Used by cyber actors during August 25-26, 2022 while attempting to exploit CVE-2022-27925 and CVE-2022-37042
185.112.83[.]77	**New September 27, 2022:** Used by cyber actors during August 25-26, 2022 while attempting to exploit CVE-2022-27925 and CVE-2022-37042
207.148.76[.]235	A Cobalt Strike command and control (C2) domain

209.141.56[.]190	**New September 27, 2022**

alert tcp any any -> any any (msg:"ZIMBRA: HTTP POST content data '.jsp' file'"; sid:x; flow:established,to_server; content:"POST"; http_method; content:"|2f|service|2f|extension|2f|backup|2f|mboximport"; nocase; http_uri; content:"file|3a|"; nocase; http_client_body; content:"|2e|jsp"; http_client_body; fast_pattern; classtype:http-content; reference:cve,2022-30333;)
alert tcp any any -> any any (msg:"ZIMBRA: Client HTTP Header 'QIHU 360SE'"; sid:x; flow:established,to_server; content:"POST"; http_method; content:"|2f|service|2f|extension|2f|backup|2f|mboximport"; nocase; http_uri; content:"QIHU|20|360SE"; nocase; http_header; fast_pattern; classtype:http-header; reference:cve,2022-30333;)
alert tcp any any -> any any (msg:"ZIMBRA:HTTP GET URI for Zimbra Local Config"; sid:x; flow:established,to_server; content:"/public/jsp/runas.jsp?pwd=zim&i=/opt/zimbra/bin/zmlocalconfig|3a|-s"; http_uri; classtype:http-uri; reference:cve,2022-30333;)

- Deploy third-party YARA rules to detect malicious activity:
  - Volexity's Mass Exploitation of (Un)authenticated Zimbra RCE: CVE-2022-27925

Recommendations:

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 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 (MFA) for all users and virtual private network (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. **Reimage 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 detailed operational procedures for planning and conducting cybersecurity incident and vulnerability response activities.

Reference(s)	CISA, Volexity, GitHub

Recommendations

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

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

YARA Rules

Alert ID 1bf9e7aa

This Alert has 2 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

Download Health-ISAC's Information Sharing App.

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