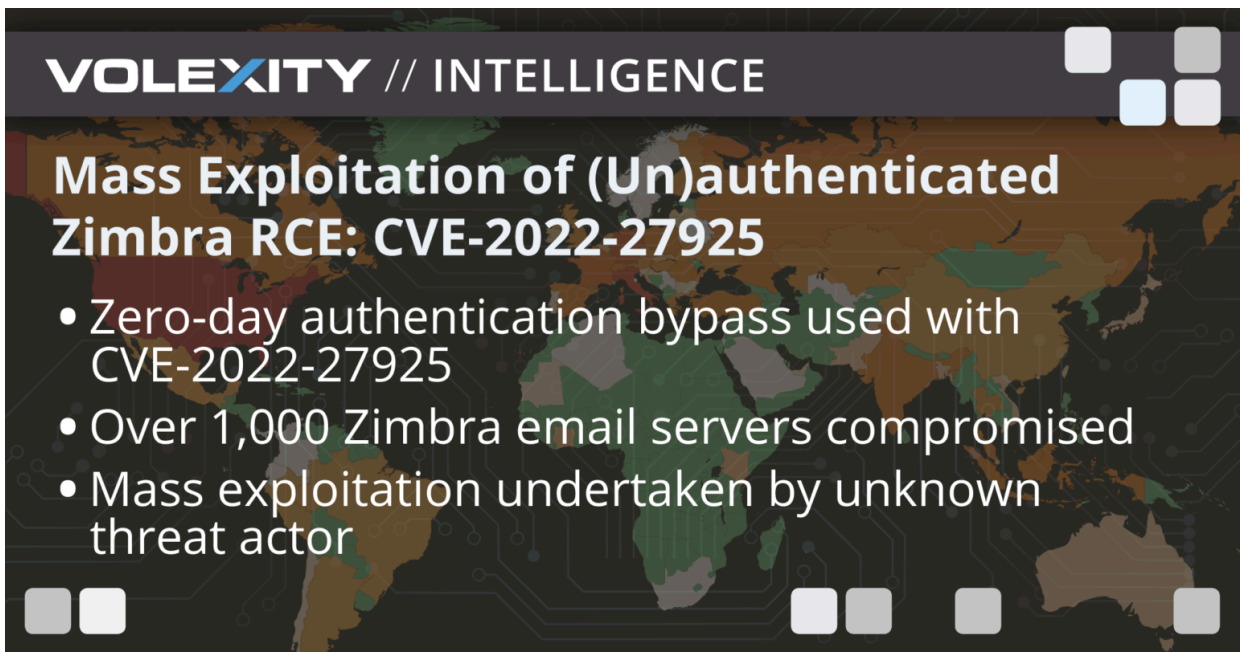
Mass Exploitation of (Un)authenticated Zimbra RCE: CVE-2022-27925

AUGUST 10, 2022

by Volexity Threat Research



[Note: Volexity has reported all findings in this post to Zimbra. Where an existing contact was known, Volexity has notified local CERTs of compromised Zimbra instances in their constituency. The newest versions of Zimbra are patched for both the RCE vulnerability and authentication bypass vulnerabilities described in this blog.]

In July and early August 2022, Volexity worked on multiple incidents where the victim organization experienced serious breaches to their Zimbra Collaboration Suite (ZCS) email servers. Volexity's investigations uncovered evidence indicating the likely cause of these breaches was exploitation of CVE-2022-27925, a remote-code-execution (RCE) vulnerability in ZCS. This initial CVE was patched by Zimbra in March 2022 in 8.8.15P31 and 9.0.0P24.

CVE-2022-27925 Detail

Current Description

Zimbra Collaboration (aka ZCS) 8.8.15 and 9.0 has mboximport functionality that receives a ZIP archive and extracts files from it. An authenticated user with administrator rights has the ability to upload arbitrary files to the system, leading to directory traversal.

Figure 1. Description of CVE-2022-27925 from the NIST website

Initial research into the vulnerability did not uncover any public exploit code, but since a patch had been available for several months, it was reasonable that exploit code could have been developed based on the description of the vulnerability. However, one thing that caught Volexity's attention was that, beyond being remotely executable, the

SEARCH

RECENT POSTS

StormBamboo Compromises ISP to Abuse Insecure Software Update Mechanisms

DISGOMOJI Malware Used to Target Indian Government

Detecting Compromise of CVE-2024-3400 on Palo Alto Networks GlobalProtect Devices

Zero-Day Exploitation of Unauthenticated Remote Code Execution Vulnerability in GlobalProtect (CVE-2024-3400)

CharmingCypress: Innovating Persistence

ARCHIVES

August 2024
June 2024
May 2024
April 2024
February 2024
January 2024
September 2023
June 2023
March 2023
December 2022
August 2022
July 2022

vulnerability description clearly stated its exploitation required valid administrator credentials. This added a significant level of difficulty for an attacker to successfully compromise a ZCS instance and made mass exploitation unlikely.

As each investigation progressed, Volexity found signs of remote exploitation but no evidence the attackers had the prerequisite authenticated administrative sessions needed to exploit it. Further, in most cases, Volexity believed it extremely unlikely the remote attackers would have been able to obtain administrative credentials on the victims' ZCS email servers.

As a result of the above findings, Volexity initiated more research into determining a means to exploit CVE-2022-27925, and if it was possible to do so without an authenticated administrative session. Subsequent testing by Volexity determined it was possible to bypass authentication when accessing the same endpoint (`mboximport`) used by CVE-2022-27925. This meant that CVE-2022-27925 could be exploited **without** valid administrative credentials, thus making the vulnerability significantly more critical in severity.

Volexity reported these findings to Zimbra, and Zimbra patched the authentication issue in its 9.0.0P26 and 8.8.15P33 releases at the end of July. The authentication bypass vulnerability was assigned **CVE-2022-37042.**

Through multiple investigations, evidence was uncovered indicating that CVE-2022-27925 was being mass exploited with the authentication bypass as early the end of June 2022. Volexity believes this vulnerability was exploited in a manner consistent with what it saw with Microsoft Exchange 0-day vulnerabilities it discovered in early 2021. Initially it was exploited by espionage-oriented threat actors, but was later picked up by other threat actors and used in mass-exploitation attempts.

Based on what was learned from investigating these attacks, Volexity performed Internet-wide scans to identify compromised Zimbra instances belonging to non-Volexity customers. Through these scans, Volexity identified over 1,000 ZCS instances around the world that were backdoored and compromised (Figure 2). These ZCS instances belong to a variety of global organizations, including government departments and ministries; military branches; worldwide businesses with billions of dollars of revenue; etc. At the other end of the scale, the affected organizations also included a significant number of small businesses unlikely to have dedicated IT staff to manage their mail servers, and perhaps less likely to be able to effectively detect and remediate an incident.

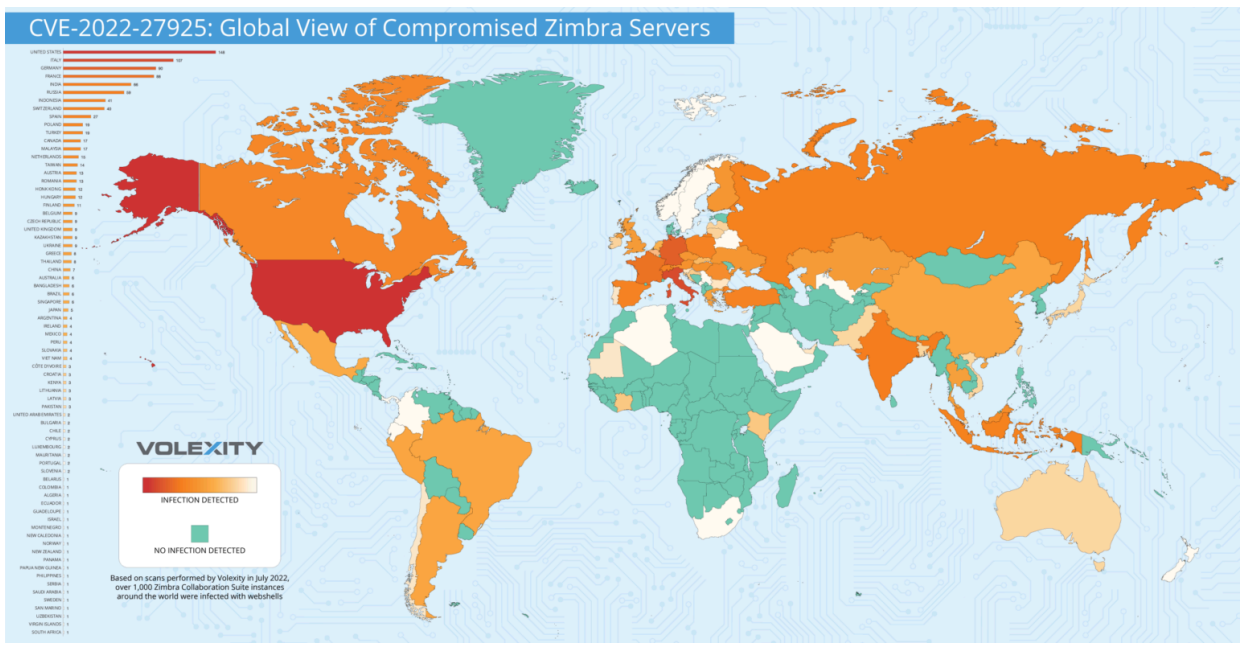


Figure 2. Geographic distribution of compromised Zimbra servers (by geolocation of IP)

This post details how the authentication bypass for CVE-2022-27925 works and gives details of the various paths to shells identified by Volexity that are indicative of compromise of ZCS instances.

June 2022
March 2022
February 2022
December 2021
August 2021
May 2021
March 2021
December 2020
November 2020
April 2020
March 2020
September 2019
November 2018
September 2018
August 2018
July 2018
June 2018
April 2018
November 2017
July 2017
March 2017
November 2016
October 2015
July 2015
June 2015
April 2015
October 2014
September 2014

TAGS

China exploits Exploit memory forensics VPN phishing webshell Scanning osx vulnerabilities pulsesecure 0day APT malware crimeware ivanti connect secure RCE spear phishing Threat Intelligence North Korea

Analysis

While investigating the compromise of multiple Zimbra email server instances as part of incident response activities, Volexity confirmed remote exploitation of ZCS as the root cause of multiple incidents. The next step was to identify the version of ZCS to determine if there were any known vulnerabilities that would allow for an easy breach by a threat actor. In each case, the servers in question were not fully up to date with patches and, in most cases, were behind by only a single patch. However, there were no known unauthenticated remote-code-execution (RCE) vulnerabilities for these instances known to be in the wild.

Inspecting the web logs from compromised servers often turned over evidence of exploitation consistent with this vulnerability prior to a webshell being written to disk. An example web log entry is shown below.

> [attacker_ip] - - [30/Jun/2022:05:33:18 +0000] "POST [snipped]/service/extension/backup/mboximport?account-name=admin&ow=1&no-switch=true HTTP/1.0" 401 299 "[snipped]" "Mozilla/5.0 (X11; Linux x86_64; rv:101.0) Gecko/20100101 Firefox/101.0" 7

At first glance, these seemed like open-and-shut cases that immediately proved the ZCS servers were compromised via CVE-2022-27925. However, as previously noted, the description of the CVE suggested that an authenticated administrator account was required for exploitation. Volexity combed through logs, memory samples, and other data to determine if the attacker somehow had valid administrative credentials. In each instance, there was no evidence to support or suggest the attackers had obtained or used such credentials.

To investigate further and attempt to replicate the exploit, Volexity set up a test instance of ZCS and followed online write-ups describing the vulnerability. Volexity found two write-ups published on Chinese websites detailing the inner workings of CVE-2022-27925. The first write-up was dated June 13, 2022, and predated all observed exploit activity. The second write-up contained more detail on how to exploit the vulnerability; it was published on July 7, 2022, well after many cases of public exploitation.

For testing, the following steps were taken:

- Set up a vulnerable instance of ZCS.
- Create a specially crafted ZIP file containing a file with a name that contains a relative path, allowing it to be dropped to the correct directory.
- Send an HTTP POST request to the ZCS instance's MailboxImport servlet with the ZIP file in the body of the post.
- Use an authentication token belonging to a logged-in administrator in the correct HTTP header (this can be done by logging in and inspecting requests manually) to authenticate with the server.

While following these steps, Volexity initially tried the request without an administrator authentication token. Although an HTTP response was received indicating the request had failed, the webshell content was correctly placed in the intended path on the test server. Taking a second look at the logs from successful exploitation in the incident, Volexity saw the attacker also got a 401 (Unauthorized) status code when uploading their webshell.

Inspecting the source code for the `MailboxImport` servlet yielded immediate answers. The "doPost" function is called when this URL is hit, which immediately checks if the user is authenticated (Figure 3).

Figure 3: The beginning of the "MailboxImport" servlet function

The problem with this code is that authentication is checked and an error message is set, but there is no return statement. This means subsequent code will continue to be executed, irrespective of the user's authentication state. Following the function down, an attacker only needs to set the correct parameters in the URL in order to exploit the vulnerability.

In summary, an unauthenticated user was able to access this endpoint (which is intended as a feature used by administrators), and further means that CVE-2022-27925 can effectively be turned into an **unauthenticated** RCE exploit. Even after the patch for CVE-2022-27925, which fixed the directory traversal issue, an attacker could overwrite any user's mailbox using a specially crafted request, as the initial patch did not resolve the authentication issue. This has since been patched by Zimbra.

Possible Widespread Exploitation

During the incidents which led to this discovery, Volexity determined that attackers often deployed a number of webshells to gain persistent access to the ZCS servers; each of these webshells created a new file on the server that did not previously exist and a new URL the attacker could access to interact with the webshell. In ZCS, if a request is made to a URL that does not exist, it will respond with a "404 Not Found" response; however, once a webshell is placed, the behavior when accessing a given URI is changed depending on the logic present in the webshell. Often, these webshells do not have logic to handle the case where requests are made that are not in accordance with the logic of the webshell's design, and thus respond with a "200 OK" status code with a 0-byte response.

Knowing the paths to which the attacker had installed webshells, and the behavior of ZCS when contacting a URL that did not exist, Volexity performed a scan of ZCS instances in the wild to identify third-party compromises using the same webshell names. This scan yielded over 1,000 infected ZCS instances worldwide. Bearing in mind that this scan only used shell paths known to Volexity, **it is likely that the true number of compromised servers is higher**. The table below shows the top 10 countries with the most compromised servers discovered in this scan:

Country	# IP addresses hosting webshells
US	148
IT	107
DE	90
FR	88
IN	66
RU	59
ID	41
CH	40
ES	27

PL	19

It is worth noting that often the compromised organization may be based in a country that differs from where the ZCS instance is hosted, as these statistics are based on the IP address geolocation.

Identifying Compromise & Webshells

In each incident, irrespective of whether it was believed to be the work of a dedicated attacker or widespread compromise, Volexity observed a variety of webshells deployed by different attackers exploiting this vulnerability. None of these webshells deployed are particularly novel techniques, and a large number of them were available on GitHub.

In order to verify the presence of webshells on a ZCS instance, one technique that can be used is to compare the list of JSP files on a Zimbra instance with those present by default in Zimbra installations. Lists of valid JSP files included in Zimbra installations are given here for the latest version of 8.8.15 and of 9.0.0.

Conclusion

CVE-2022-27925 was originally listed as an RCE exploit requiring authentication. When combined with a separate bug, however, it became an unauthenticated RCE exploit that made remote exploitation trivial. Some organizations may prioritize patching based on the severity of security issues. In this case, the vulnerability was listed as medium—not high or critical—which may have led some organizations to postpone patching.

These cases highlight a general issue with web-facing appliances or software. When an RCE exploit becomes available, any compromise that occurs between the exploit becoming available and the patch being available is not remediated by the provider of the web-facing appliances. While patching appliances or software to the newest version may provide safety from future exploitation, it does not remediate historic compromise. When applying patches to systems that have been vulnerable—especially to an RCE exploit—a proactive threat assessment should be performed to verify no exploitation occurred in the time between a patch becoming available and being applied.

Volexity notified Zimbra of the authentication issue with this endpoint and its impact on the original CVE-2022-27925. Zimbra has patched the authentication issue in its 9.0.0P26 and 8.8.15P33 releases.

It is interesting to note that CVE-2022-27925 may not be the only exploit for ZCS that is being actively used by attackers. The Cybersecurity and Infrastructure Agency (CISA) posted an advisory on August 4, 2022, warning of exploitation of a credential-theft vulnerability, CVE-2022-27924, likely in relation to other active incidents involving breaches beginning with ZCS compromise.

If your organization runs ZCS and did not apply patches 8.8.15P31 or 9.0.0P24 before the end of May 2022, you should consider your ZCS instance may be compromised (and thus all data on it, including email content, may be stolen) and perform a full analysis of the server. This could include, but is not limited to, the following steps:

- Perform an initial memory acquisition to preserve any memory-resident traces of attacker activity.
- Look in logs for any requests with 40x-based status codes to the vulnerable servlet `/service/extension/backup/mboximport`.

- Thoroughly inspect the Zimbra users directory (usually `/opt/zimbra/`) to identify possible webshells and any other evidence of exploitation.
- Use the YARA rules provided here to identify related webshells.
- Look for inbound requests to your ZCS server to JSP files matching paths **not** listed in the corresponding 8.8.15 and 9.0.0 valid JSP files here.

Based on limited testing by Volexity, it seems that patching ZCS instances to the newest version may remove webshells placed in some directories. However, if an attacker installed any second-stage or persistent malware (run via cron), then patching your ZCS instance is insufficient to remediate the compromise. **If you believe your ZCS server may have been compromised, and you need assistance investigating a possible incident, please feel free to contact Volexity for assistance**.

If your organization is not able to perform incident response, or if you are not able to engage a third party for incident response, then Volexity advises the following:

- Rebuild your ZCS instance using the latest patch
- Import Mail from the old server to the new server.

Zimbra has a guide on the steps to do this here.

The information surrounding the exploitation of CVE-2022-27925 and CVE-2022-37042 was shared with Volexity Threat Intelligence customers in TIB-20220802.

0day, cve-2022-27925, Exploit, webshell, Zimbra