

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Critical Command Execution Flaw in Zimbra Under Active Exploitation

Date of Publication

October 7, 2024

Admiralty Code

A1

TA Number

TA2024382




Summary

First Seen: September 4, 2024

Affected Product: Synacor Zimbra Collaboration

Impact: CVE-2024-45519 is a critical vulnerability in the Zimbra Collaboration Suite that allows unauthenticated remote command execution due to an OS command injection flaw in the postjournal service. The vulnerability has been actively exploited, with attackers installing web shells and executing arbitrary commands. Exploitation risks include privilege escalation and full system compromise, making it crucial for organizations to apply patches immediately or disable the postjournal service if not needed.

CVE

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | CISA KEV | PATCH |
|----------------|--|------------------------------|---|---|---|
| CVE-2024-45519 | Synacor Zimbra Collaboration Command Execution Vulnerability | Synacor Zimbra Collaboration |  |  |  |

Vulnerability Details

#1

CVE-2024-45519 is a critical vulnerability identified in the Zimbra Collaboration Suite (ZCS), a widely used cloud-based collaboration and email platform. This vulnerability allows for unauthenticated remote command execution due to an OS command injection flaw in the postjournal service, which handles email archiving. Attackers can exploit the flaw by sending specially crafted SMTP messages that inject arbitrary commands into vulnerable systems, even without requiring authentication. This poses a serious risk to organizations using Zimbra.

#2

The affected versions include ZCS prior to 8.8.15 Patch 46, 9 before 9.0.0 Patch 41, 10 before 10.0.9, and 10.1 before 10.1.1. The issue stems from unsanitized user input being passed to the popen function within the postjournal service. This lack of input validation allows attackers to inject malicious commands, potentially leading to unauthorized access, privilege escalation, and compromise of the system's integrity and confidentiality.

#3

Exploitation of CVE-2024-45519 has been observed in the wild since late September 2024, shortly after Zimbra released patches addressing the flaw. Attackers are using this vulnerability to install web shells and execute commands remotely.

#4

Multiple Proof of Concept (PoC) exploits are publicly available, demonstrating the feasibility of remote exploitation without authentication. Over 19,600 systems remain unpatched, with high numbers in the U.S., Germany, and Russia. The active exploitation of this vulnerability underscores the urgency for organizations to patch affected systems immediately.

#5

Zimbra has released updates that address the flaw by sanitizing user input and replacing the vulnerable popen function with execvp. Administrators are urged to apply these updates as soon as possible. Additionally, for environments where the postjournal service is not required, temporarily disabling or removing the service can further mitigate risks until patching is complete.

Vulnerabilities

| CVE ID | AFFECTED PRODUCTS | AFFECTED CPE | CWE ID |
|----------------|--|--|--------------------|
| CVE-2024-45519 | Zimbra Collaboration (ZCS) before 8.8.15 Patch 46, 9 before 9.0.0 Patch 41, 10 before 10.0.9, and 10.1 before 10.1.1 | cpe:2.3:a:zimbra:collaboration:*:*:*:*:*:* | CWE-863 CWE-284 |

Recommendations



Apply Patches and Updates: Ensure that all instances of ZCS are updated to versions that include the patches for CVE-2024-45519.



Disable Postjournal Service: If the postjournal service is not needed for your organization's operations, consider disabling or removing it entirely to reduce the attack surface.



Network Segmentation and Least Privilege: Segment critical systems and restrict network access to them. Implementing the principle of least privilege ensures that even if an attacker gains access through this vulnerability, their ability to move laterally within your network will be limited. This reduces the overall damage potential.



Conduct Security Audits: Regularly audit your Zimbra instance for vulnerabilities and misconfigurations. Use automated vulnerability scanners to detect known issues and test for the presence of CVE-2024-45519.



Verify Network Configuration: Ensure that the mynetworks parameter is configured securely to restrict access only to trusted internal networks. Misconfigured settings may allow attackers to bypass restrictions and exploit the vulnerability remotely.



Potential MITRE ATT&CK TTPs

| | | | |
|--|--|--|--|
| <u>TA0001</u> Initial Access | <u>TA0042</u> Resource Development | <u>TA0002</u> Execution | <u>TA0004</u> Privilege Escalation |
| <u>T1059</u> Command and Scripting Interpreter | <u>T1588.006</u> Vulnerabilities | <u>T1588</u> Obtain Capabilities | <u>T1588.005</u> Exploits |
| <u>T1203</u> Exploitation for Client Execution | <u>T1190</u> Exploit Public-Facing Application | <u>T1068</u> Exploitation for Privilege Escalation | |

✂ Indicator of Compromise (IOCs)

| TYPE | VALUE |
|------|--------------------|
| IPv4 | 79[.]124[.]49[.]86 |

Patch Details

Upgrade Zimbra Collaboration Suite (ZCS) to the fixed versions as below mentioned:

- ZCS 8.8.15 Patch 46 or later
- ZCS 9.0.0 Patch 41 or later
- ZCS 10.0.9 or later
- ZCS 10.1.1 or later

Links:

https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P46

https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P41

https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.9

https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.1

References

<https://blog.zimbra.com/2024/10/zimbra-cve-2024-45519-vulnerability-stay-secure-by-updating/>

<https://www.fortiguard.com/threat-signal-report/5553/synacor-zimbra-collaboration-command-execution-vulnerability-cve-2024-45519>

<https://x.com/JusticeRage/status/1841017884245438555>

<https://blog.projectdiscovery.io/zimbra-remote-code-execution/>

<https://x.com/Shadowserver/status/1842634837532070356>

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 7, 2024 • 7:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com