

THREAT ADVISORY



**VULNERABILITY
REPORT**

Vulnerability in Zimbra that steals clear-text credentials from users

Date of Publication

June 21, 2022

Admiralty code

A1


TA Number

TA2022129

Summary

A new vulnerability in Zimbra allows an attacker to steal cleartext credentials from instances via Memcache injection. Over 200,000 users logged in can be impacted by the security flaw

CVEs

CVE	NAME	PATCH
CVE-2022-27924	Memcached poisoning with unauthenticated request	

Potential MITRE ATT&CK TTPs

TA0004 Privilege Escalation	TA1068 Exploitation for Privilege Escalation	TA0011 Command and Control	TA0006 Credential Access
T1539 Steal Web Session Cookie	T1090 Proxy		

Technical Details

- #1** The Zimbra Collaboration helps unauthenticated attackers to inject arbitrary memcache commands into a targeted instance, which then becomes unescaped and causes an overwrite of cached entries.
- #2** In order to exploit this vulnerability, the attacker might require the victim's email address and poison the cache to steal the login credentials.
- #3** An alternative exploitation technique, exploits "Response Smuggling" to bypass any restrictions imposed by the first strategy and allows an attacker to steal cleartext credentials from any vulnerable Zimbra instance. Both strategies require no user interaction

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-27924	8.8.15 and 9.0 branches of Zimbra	cpe:2.3:a:zimbra:collaboration:8.8.15:-:*:*:*:*:* cpe:2.3:a:zimbra:collaboration:9.0.0:-:*:*:*:*:*	CWE-74

Patch Details

Zimbra patched the vulnerability by creating a SHA-256 hash of all Memcache keys before sending them to the Memcache server.

- 9.0.0 Patch 24
- 8.8.15 Patch 31

Patch Link

https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P31.1

References

<https://blog.sonarsource.com/zimbra-mail-stealing-clear-text-credentials-via-memcache-injection/>

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.



At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

June 21, 2022 • 4:30 AM

© 2022 All Rights are Reserved by HivePro



More at www.hivepro.com