Hive Pro

THREAT ADVISORY

Zero-day vulnerability in Zimbra Servers being exploited-in-the-wild	**TA2022043**
Threat Level RED	**Publish Date –** March 1, 2022

A zero-day cross-site scripting (XSS) vulnerability has been discovered in the Zimbra email software. A threat actor is taking advantage of this issue by launching a targeted spear-phishing attack named Operation EmailThief.

Two attack phases make up the Operation EmailThief campaign. The first phase was intended for reconnaissance, and it consisted of emails designed to simply track whether a target had received and opened the emails. The second phase targets users to click on a maliciously created link by the attacker. This attack can only succeed if the victim is using a web browser to access their Zimbra webmail client. If exploited successfully, an attacker will be able to run arbitrary JavaScript in the context of a user's Zimbra session, then exfiltrate the data to the attacker's C2 server.

This vulnerability has been exploited in the wild and organizations should upgrade to version 8.8.15 P30(update 1) to fix it.

Potential MITRE ATT&CK TTPs are:
TA0043: Reconnaissance
T1589: Gather Victim Identity Information
T1589.002: Gather Victim Identity Information: Email Addresses
TA0001: Initial Access
T1566: Phishing
T1566.002: Phishing: Spearphishing Link
T1189: Drive-by Compromise
TA0002: Execution
T1204: User Execution
T1204.001: User Execution: Malicious Link
T1059: Command and Scripting Interpreter
T1059.007: Command and Scripting Interpreter: JavaScript
TA0010: Exfiltration
T1041: Exfiltration Over C2 Channel

Vulnerability Detail

CVE ID	Affected Version	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-24682	8.8 to 8.8.15	cpe:2.3:a:zimbra:collaboration:*:*:*:*:*:*:*:*	Zimbra Collaboration Suite cross-site Scripting vulnerability	CWE-79

Indicators of Compromise (IoCs)

Type	Value
IPV4	206.166.251.141 206.166.251.166 108.160.133.32 172.86.75.158

Type	Value
Hostname	iceywindflow.ml news-voice.ml bruising-intellect.ml thunderchannel.tk spiritfield.ml iceywindflow.cf thunderchannel.cf spiritfield.tk update.secretstep.tk mail.bruising-intellect.ml www.news-online.ml www.thunderchannel.cf www.spiritfield.ga winderosion.spiritfield.ml flameshock.spiritfield.tk windsource.thunderchannel.cf yahoo-movie.spiritx.ga windsource.thunderchannel.tk opticaleel.iceywindflow.cf shadownight.spiritfield.ga www.yahoo-corporation.ml amazon-check.gq amazon-team.tk yahoo-corporation.ml playquicksand.gq yahoo-corporation.tk playquicksand.cf spiritfield.cf amazon-check.ga amazon-check.cf amazon-check.tk playquicksand.ml www.playquicksand.cf www.amazon-check.ga www.playquicksand.gq www.iceywindflow.gq chargedboltsentry.spiritfield.tk newsonline.gq spiritx.ga secretstep.tk spiritfield.ga www.news-voice.ml www.findtruth.ml

Type	Value
Hostname	www.newsonline.gq mx.newsonline.gq www.spiritx.ga support.newsonline.gq www.thunderchannel.tk windsoft.cf findtruth.ml news-online.ml iceywindflow.gq shadownight.playquicksand.tk www.windsoft.cf tigerstrike.iceywindflow.ml shadowmaster.iceywindflow.ml playquicksand.tk

Patch Link

https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P30

References

https://www.volexity.com/blog/2022/02/03/operation-emailthief-active-exploitation-of-zero-day-xss-vulnerability-in-zimbra/
https://blog.zimbra.com/2022/02/hotfix-available-5-feb-for-zero-day-exploit-vulnerability-in-zimbra-8-8-15/