F#RTINET.

OUTBREAK ALERTS





Synacor Zimbra Collaboration MBoxImport **Vulnerabilities**

Zimbra Collaboration aka (ZCS) Authentication Bypass in MailboxImportServlet functionality and Arbitrary File Upload Vulnerability. https://wiki.zimbra.com/wiki/Zimbra Security Advisories

CVEs: CVE-2022-37042, CVE-2022-27925

Zimbra Collaboration Suite (ZCS) 8.8.15 and 9.0 has mboximport functionality that receives a ZIP archive and extracts files. By bypassing authentication, an attacker can upload arbitrary files to the system, leading to directory traversal and remote code execution. The vulnerability exists due to an incomplete fix for CVE-2022-27925.

> Zimbra Collaboration is the trusted email and collaboration platform and productivity suite that includes contacts, calendar, tasks, chat and file sharing, etc. According to Zimbra's blog, the Collaboration software is used in more

Collaboration that is actively leveraged in the field by threat actors. The advisory covers five CVEs: CVE-2022-

Announced 8/10/2022: Zimbra blog posted

https://blog.zimbra.com/2022/08/authentication-bypass-in-mailboximportservlet-vulnerability/

than 140 countries and over 1,000 government and financial institutions.

Latest Developments

8/16/2022: A joint cybersecurity advisory was issued by the Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC) on vulnerabilities in Zimbra

24682, CVE-2022-27924, CVE-2022-27925, CVE-2022-37042, and CVE-2022-30333. CISA advisory: https://www.cisa.gov/uscert/ncas/alerts/aa22-228a



Background

events:

PROTECT

Reconnaissance

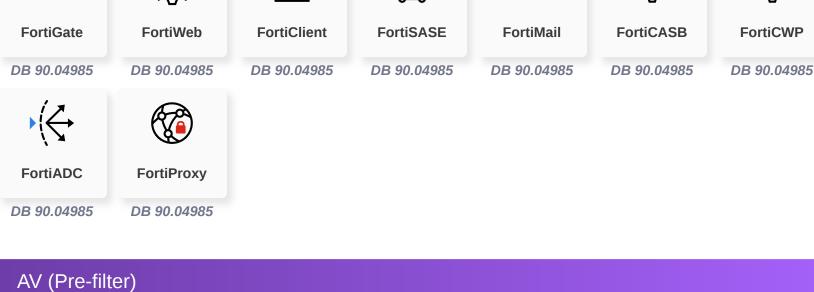
Countermeasures across the security fabric for protecting assets, data and network from cybersecurity

Weaponization

AV

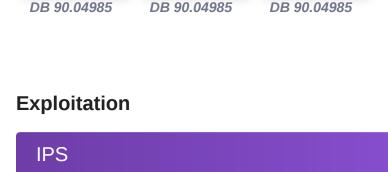
Blocks malware exploiting the Zimbra Collabolation vulnerabilities (CVE-2022-27925, CVE-2022-37042)

Delivery



FortiEDR FortiSandbox FortiNDR

Blocks malware exploiting the Zimbra Collabolation vulnerabilities(CVE-2022-27925, CVE-2022-37042)



FortiGate

DB 21.376

Web App Security

Blocks attack attempts related to Zimbra Collaboration vulnerabilities (CVE-2022-27925 CVE-2022-37042)

Blocks attack attempts related to Zimbra Collaboration vulnerabilities (CVE-2022-27925 CVE-2022-37042)



Action



Outbreak Detection

DETECT

alert and generate reports:

FortiAnalyzer

Find and correlate important information to identify an outbreak, the following updates are available to raise



Content Update

Threat Hunting

DB 1.00059



RESPOND

Automated Response

FortiXDR

Develop containment techniques to mitigate impacts of security events:

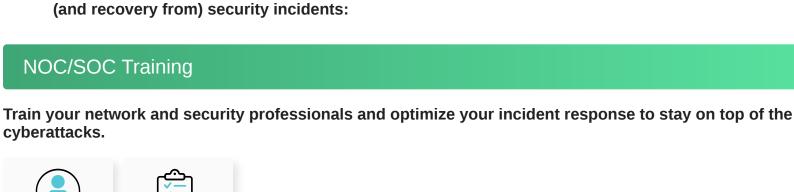


Assisted Response Services Experts to assist you with analysis, containment and response activities.

RECOVER

Response

Services that can automatically respond to this outbreak.



NSE Training

Readiness **End-User Training**

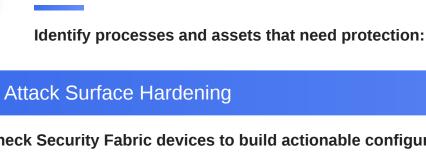
and other forms of cyberattacks.

Response

Awareness & **Training**

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download

Improve security posture and processes by implementing security awareness and training, in preparation for



Check Security Fabric devices to build actionable configuration recommendations and key indicators.

IDENTIFY

Rating



Volexity

Bleeping Computer

Threat Signal

Security

Additional Resources

https://www.volexity.com/blog/2022/08/10/mass-exploitation-of-unauthenticated-zimbra-rce-cve-2022-27925/

https://www.bleepingcomputer.com/news/security/zimbra-auth-bypass-bug-exploited-to-breach-over-1-000-servers/

The Hacker News https://thehackernews.com/2022/08/researchers-warn-of-ongoing-mass.html

https://www.fortiguard.com/threat-signal-report/4714

Learn more about FortiGuard Outbreak Alerts

F