FORTINET

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.

Background

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

Announced

8/10/2022: Zimbra blog posted
https://blog.zimbra.com/2022/08/authentication-bypass-in-mailboximportservlet-vulnerability/

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 Collaboration that is actively leveraged in the field by threat actors. The advisory covers five CVEs: CVE-2022-24682, CVE-2022-27924, CVE-2022-27925, CVE-2022-37042, and CVE-2022-30333. CISA advisory:
https://www.cisa.gov/uscert/ncas/alerts/aa22-228a

PROTECT

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

- Reconnaissance
- Weaponization
- Delivery

AV

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

FortiGate	FortiWeb	FortiClient	FortiSASE	FortiMail	FortiCASB	FortiCWP
DB 90.04985	DB 90.04985	DB 90.04985	DB 90.04985	DB 90.04985	DB 90.04985	DB 90.04985

FortiADC	FortiProxy
DB 90.04985	DB 90.04985

AV (Pre-filter)

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

FortiEDR	FortiSandbox	FortiNDR
DB 90.04985	DB 90.04985	DB 90.04985

- Exploitation

IPS

Blocks attack attempts related to Zimbra Collaboration 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)

FortiWeb	FortiADC
DB 0.00327	DB 1.00036

- Installation
- C2
- Action

DETECT

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

Outbreak Detection

FortiAnalyzer
DB 1.00059

Threat Hunting

FortiAnalyzer	FortiSIEM
v7.0+	DB 6.4.0+

Content Update

FortiSIEM
DB 302

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

Assisted Response Services

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

Incident Response

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

NSE Training	Response Readiness

End-User Training

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download and other forms of cyberattacks.

Security Awareness & Training

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

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

Security Rating

Additional Resources

Volexity	https://www.volexity.com/blog/2022/08/10/mass-exploitation-of-unauthenticated-zimbra-rce-cve-2022-27925/
Bleeping Computer	https://www.bleepingcomputer.com/news/security/zimbra-auth-bypass-bug-exploited-to-breach-over-1-000-servers/
Threat Signal	https://www.fortiguard.com/threat-signal-report/4714
The Hacker News	https://thehackernews.com/2022/08/researchers-warn-of-ongoing-mass.html

Learn more about FortiGuard Outbreak Alerts

FORTINET