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

Cyber Kill Chain

Reconnaissance

Weaponization

Delivery

FortiGate
AV 90.04985
Blocks malware exploiting the Zimbra Collaboration vulnerabilities (CVE-2022-27925, CVE-2022-37042)

FortiWeb
AV 90.04985
Blocks malware exploiting the Zimbra Collaboration vulnerabilities (CVE-2022-27925, CVE-2022-37042)

FortiClient
AV 90.04985
Blocks malware exploiting the Zimbra Collaboration Vulnerabilties (CVE-2022-27925, CVE-2022-37042)

FortiEDR
AV (Pre-Filter) 90.04985
Blocks malware exploiting the Zimbra Collaboration vulnerabilities(CVE-2022-27925, CVE-2022-37042)

FortiSASE
AV 90.04985
Blocks malware exploiting the Zimbra Collaboration vulnerabilities(CVE-2022-27925, CVE-2022-37042)

FortiSandbox
AV (Pre-Filter) 90.04985
Blocks malware exploiting the Zimbra Collaboration vulnerabilities(CVE-2022-27925, CVE-2022-37042)

FortiNDR
AV (Pre-Filter) 90.04985
Blocks malware exploiting the Zimbra Collaboration vulnerabilities(CVE-2022-27925, CVE-2022-37042)

FortiMail
AV 90.04985
Blocks malware exploiting the Zimbra Collaboration vulnerabilities(CVE-2022-27925, CVE-2022-37042)

FortiCASB
AV 90.04985
Blocks malware exploiting the Zimbra Collaboration vulnerabilities(CVE-2022-27925, CVE-2022-37042)

FortiCWP
AV 90.04985
Blocks malware exploiting the Zimbra Collaboration vulnerabilities(CVE-2022-27925, CVE-2022-37042)

FortiADC
AV 90.04985
Blocks malware exploiting the Zimbra Collaboration vulnerabilities(CVE-2022-27925, CVE-2022-37042)

FortiProxy
AV 90.04985
Blocks malware exploiting the Zimbra Collaboration vulnerabilities(CVE-2022-27925, CVE-2022-37042)

Exploitation

FortiGate
IPS 21.376
Blocks attack attempts related to Zimbra Collaboration vulnerabilities (CVE-2022-27925 CVE-2022-37042)

FortiWeb
Web App Security 0.00327
Blocks attack attempts related to Zimbra Collaboration vulnerabilities (CVE-2022-27925 CVE-2022-37042)

FortiSASE
IPS 21.376
Blocks attack attempts related to Zimbra Collaboration vulnerabilities (CVE-2022-27925 CVE-2022-37042)

FortiNDR
IPS 21.376
Blocks attack attempts related to Zimbra Collaboration vulnerabilities (CVE-2022-27925 CVE-2022-37042)

FortiADC
IPS 21.376
Blocks attack attempts related to Zimbra Collaboration vulnerabilities (CVE-2022-27925 CVE-2022-37042)

Web App Security 1.00036
Blocks attack attempts related to Zimbra Collaboration vulnerabilities (CVE-2022-27925 CVE-2022-37042)

FortiProxy
IPS 21.376
Blocks attack attempts related to Zimbra Collaboration vulnerabilities (CVE-2022-27925 CVE-2022-37042)

Installation

C2

Action

Endpoint

Incident Response (Security Operations)

To help customers identify and protect vulnerable, FortiAnalyzer, FortiSIEM and FortiSOAR updates are available to raise alerts and escalate to incident response:

FortiAnalyzer

Outbreak Detection Version 1.059
https://www.fortiguard.com/updates/outbreak-detection-service?version=1.00059

Threat Hunting Version 7.0
https://community.fortinet.com/t5/FortiAnalyzer/Technical-Tip-Using-FortiAnalyzer-to-detect-Zimbra-Collaboration/ta-p/221810

FortiSIEM

Content Update Version 302
https://help.fortinet.com/fsiem/6-6-0/Online-Help/HTML5_Help/content_updates.htm#Content2

Threat Hunting Version 6.4.0+
https://community.fortinet.com/t5/FortiSIEM/Technical-Tip-Using-FortiSIEM-to-detect-Synacor-Zimbra/ta-p/222009

Additional Resources

NIST Gov	https://nvd.nist.gov/vuln/detail/CVE-2022-37042
Volexity	https://www.volexity.com/blog/2022/08/10/mass-exploitation-of-unauthenticated-zimbra-rce-cve-2022-27925/
The Hacker News	https://thehackernews.com/2022/08/researchers-warn-of-ongoing-mass.html
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
CISA Advisory	https://www.cisa.gov/uscert/ncas/alerts/aa22-228a