Zimbra Vulnerability Exploited in the Wild - CVE-2024-45519

Overview

A critical vulnerability (CVE-2024-45519) affecting Zimbra Collaboration Suite has been exploited in the wild, allowing attackers to deploy web shells and execute arbitrary commands on compromised systems.

The flaw, located in Zimbra's postjournal service, stems from improper input sanitization, allowing attackers to inject malicious commands via specially crafted SMTP messages. Researchers at Proofpoint observed spoofed Gmail emails being sent to fake addresses in the CC fields in an attempt to deceive Zimbra servers into parsing and executing them as commands. The addresses contained base64-encoded strings intended to be executed by the sh utility. Exploits can occur remotely if the service is enabled and accessible within allowed network ranges.

Patched versions include:

- Zimbra 9.0.0 Patch 41
- Zimbra 10.0.9
- Zimbra 10.1.1
- Zimbra 8.8.15 Patch 46

CVE-2024-45519 was exploited just one day after the release of a Proof-of-Concept (PoC). Zimbra Collaboration Suite is widely used by thousands of organizations and serves millions of users for email, calendaring, chat, and video services. Organizations using affected Zimbra versions are strongly advised to apply patches immediately.

Aspire Protects

- **Apply Patches** - Upgrade to the latest Zimbra versions that address CVE-2024-45519. Failure to do so leaves systems vulnerable to remote code execution (RCE) attacks. Zimbra has released a patch for the vulnerability but has not released any other details. You may find patch guidance here.
- **Disable Unnecessary Services:** Ensure the postjournal service is disabled if not required.
- **Network Configuration:** Properly configure the "mynetworks" parameter to restrict access and prevent unauthorized connections.

IoCs

- Base64-encoded commands in the "CC" fields of emails.
- Web shell activity (e.g., listening on HTTP with specific cookie-based triggers like JSESSIONID).
- Malicious traffic from IP address 79[.]124[.]49[.]86.

There are no other known IoCs associated with CVE-2024-45519 at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

TTPs to Watch

- **Tactic: Initial Access (TA0001)**
  - Exploitation for Client Execution (T1203) – Attackers exploit vulnerabilities in the Zimbra postjournal service by sending specially crafted SMTP messages, allowing them to gain unauthorized access.
- **Tactic: Execution (TA0002)**
  - Command and Scripting Interpreter (T1059) – Malicious actors inject base64-encoded commands through spoofed emails to trigger command execution on vulnerable Zimbra servers.
- **Tactic: Persistence (TA0003)**
  - Web Shell (T1505.003) – Attackers deploy web shells on compromised Zimbra servers to maintain access, enabling remote execution of commands and further payload delivery.
- **Tactic: Command and Control (TA0011)**
  - Ingress Tool Transfer (T1105) – Using a pre-determined JSESSIONID cookie, attackers transfer and execute additional payloads via the web shell for remote control of the compromised system.

Aspire's Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat

- detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.

- **Aspire Managed Security Services**
  - Aspire Managed Security Services provide remote security monitoring and device management – 24 hours a day, 7 days a week. By aggregating and correlating security events from across your IT environment, our remote security monitoring service eliminates “noise” and make sense of what really matters.
  - Our managed security portfolio includes:
    - Managed Firewall
    - Managed IDS/IPS
    - Security event monitoring & incident management
    - Managed Cisco ISE (Identity Services Engine)
    - Endpoint Protection

Supporting Documentation

Zimbra Security Advisories - Zimbra :: Tech Center

Zimbra - Remote Command Execution (CVE-2024-45519) (projectdiscovery.io)