AL2024_17 Critical Exim Mail Server Vulnerability Exposes Millions to Malicious Attachments (15th July 2024)

Description

A critical vulnerability has been identified in the Exim mail transfer agent, designated as CVE-2024-39929, with a CVSS score of 9.1 out of 10. This vulnerability allows remote attackers to bypass filename extension blocking protections and potentially deliver malicious executable attachments to end-users' mailboxes.

Attack Details

This flaw enables threat actors to evade security mechanisms designed to block executable file attachments. By exploiting this vulnerability, attackers can send emails containing malicious executables directly to vulnerable Exim mail servers. Upon download or execution by unsuspecting users, these files can compromise the targeted systems, leading to potential data breaches or system takeovers.

Indicators of Compromise (IoCs):

- Vulnerable Exim mail server versions: 4.97.1 and earlier.
- Presence of multiline RFC 2231 header filenames in incoming emails.
- Suspicious email attachments with executable file extensions (.exe, .bat, .dll, etc.) delivered despite security controls.

Recommendations

1. **Upgrade Exim Mail Servers:**

   - Immediately update all Exim mail servers to version 4.98 or later, where the vulnerability has been patched.
   - Verify the integrity of the update process to ensure successful mitigation.

2. **Security Awareness and Filtering:**

   - Educate users about the risks associated with downloading and executing email attachments, especially those with executable file extensions.

- Implement strict filtering rules to block emails containing potentially malicious attachments at the perimeter.

3. **Monitor and Respond:**

   - Monitor network traffic and email logs for signs of exploitation or suspicious activities related to this vulnerability.
   - Establish incident response procedures to isolate compromised systems and investigate potential breaches quickly.

4. **Vendor and Security Community Collaboration:**

   - Stay informed about security advisories and updates from Exim project maintainers and cybersecurity communities.
   - Share threat intelligence and collaborate with peers to enhance defences against emerging threats.

Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- The Hacker News. (n.d.-b). *Critical Exim mail server vulnerability exposes millions to malicious attachments*. Retrieved from The Hacker News. https://thehackernews.com/2024/07/critical-exim-mail-server-vulnerability.html