BLACKSWAN CYBERSECURITY

THREAT ADVISORY

July 18, 2024

Exim Mail Server Flaw

SUMMARY

A critical security vulnerability has been identified in the Exim mail transfer agent, potentially allowing attackers to send malicious attachments to users' inboxes. This flaw (CVE-2024-39929) has a CVSS score of 9.1. The issue was resolved in version 4.98.

TECHNICAL DETAILS

The vulnerability stems from an improper parsing of multiline RFC2231 header filenames, enabling remote attackers to deliver malicious executable attachments to end users' mailboxes by bypassing the $mime_filename extension-blocking protection mechanism. Exim, a free mail transfer agent used on Unix and Unix-like operating systems, was first released in 1995 at the University of Cambridge.

According to Censys, there are approximately **4,830,719** public-facing SMTP mail servers running Exim. As of July 12, 2024, **1,563,085** of these Exim servers are running vulnerable versions (4.97.1 or earlier). Most of these vulnerable instances are in the U.S., Russia, and Canada. Censys stated, "*The vulnerability could allow a remote attacker to bypass filename extension blocking protection measures and deliver executable attachments directly to end-users' mailboxes. If a user were to download or run one of these malicious files, the system could be compromised.*"

For the attack to succeed, targets must click on an attached executable file. Although there are no reports of active exploitation, users must promptly apply patches to mitigate potential threats. This development comes almost a year after the maintainers of Exim addressed a set of six vulnerabilities that could lead to information disclosure and remote code execution.

RECOMMENDATIONS

- Immediately upgrade to Exim version 4.98 or later to address the vulnerability (CVE-2024-39929).
- Identify and audit all Exim servers within your network to determine which ones are running vulnerable versions (4.97.1 or earlier).
- Apply the latest security patches to all identified Exim servers to mitigate the vulnerability.
- Enable detailed logging and monitoring on Exim servers to detect any unusual activity that may indicate exploitation attempts.
- Educate users about the risks of downloading and executing attachments from unknown or untrusted sources, emphasizing the importance of cautious behavior.
- Ensure that email security policies, such as attachment filtering and extension blocking, are properly configured and enforced to prevent similar vulnerabilities from being exploited in the future.

REFERENCES

- https://nvd.nist.gov/vuln/detail/CVE-2024-39929
- https://bugs.exim.org/show_bug.cgi?id=3099#c4
- https://censys.com/cve-2024-39929/
- https://www.bleepingcomputer.com/news/security/critical-exim-bug-bypasses-security-filters-on-15-million-mail-servers/
- https://thehackernews.com/2024/07/critical-exim-mail-server-vulnerability.html