October 6, 2023

Overall rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of Exim zero-day vulnerabilities. Exim is a message transfer agent (MTA) for use on Unix systems connected to the Internet. Exim has released patches for three of the six zero-day vulnerabilities. The vulnerabilities affect versions prior to 4.96.1 and 4.97.

Technical Details

A vulnerability was discovered in Exim within the handling of NTLM challenge requests. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the service account. Authentication is not required to exploit this vulnerability. A second significant vulnerability (CVE-2023-42115) an out-of-bounds write flaw exists in Exim within the SMTP service, which listens on TCP port 25 by default. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of a buffer. An attacker can leverage this vulnerability to execute code in the context of the service account. Authentication is not required to exploit this vulnerability.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-42114, CVE-2023-42115, CVE-2023-42116, CVE-2023-42117, CVE-2023-42118, CVE-2023-42119
- USN-6411-1: Exim vulnerabilities
- Exim patches three of six zero-day bugs disclosed last week
- Six 0day exploits were filed against Exim

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: Cybersecurity Alerts