HC3: Sector Alert

May 6, 2021 TLP: White Report: 202105061600

EXIM Mail Transfer Agent (MTA) Vulnerabilities

Executive Summary

On May 4, 2021 security researchers published a collaborated report identifying 21 vulnerabilities for EXIM, an open source email server platform. These vulnerabilities can be exploited remotely and allow for full compromise of the system. Several healthcare organizations appeared in a search engine result for internet-connected devices utilizing EXIM. HC3 recommends all healthcare organizations that operate EXIM platforms immediately apply appropriate patches.

Report

In October 2020, security researchers at Qualys discovered 21 unique vulnerabilities in EXIM, an open source MTA for Unix-like operating systems. Researchers provided a proof of concept that gave a breakdown of methods to exploit. According to researchers, 10 vulnerabilities can be exploited remotely and the remaining 11 could possibly be exploited locally. Researchers warned that some of the vulnerabilities can be chained together to obtain a full remote unauthenticated code execution and gain root privileges on the EXIM Server. On May 4, 2021, a coordinated security advisory was released confirming 21 vulnerabilities affecting EXIM. Proof of concept and intricate details of vulnerabilities can be found via Qualys Report.

Analysis

Using open source resources comes with security risks because the source code is publicly available. According to a Mail (MX) Server survey, it is estimated over 59% of internet email servers run on EXIM. A recent SHODAN result of EXIM versions connected via the internet displayed several Healthcare organizations EXIM versions less than the recommended 4.94.2. Threat Actors can use these exploits to their advantage by targeting organizations that are slow to patch the applications. Russian cyber actors formally known as the Sandworm Team have also exploited EXIM vulnerabilities in the past.

Vulnerabilities

The below table summarizes all 21 vulnerabilities, both locally and remotely exploitable.

Vulnerability	Exploit
Local	
CVE-2020-28007	Link attack in Exim's log directory
CVE-2020-28008	Assorted attacks in Exim's spool directory
CVE-2020-28014	Arbitrary file creation and clobbering
CVE-2021-27216	Arbitrary file deletion
CVE-2020-28011	Heap buffer overflow in queue_run()
CVE-2020-28010	Heap out-of-bounds write in main()
CVE-2020-28013	Heap buffer overflow in parse_fix_phrase()
CVE-2020-28016	Heap out-of-bounds write in parse_fix_phrase()
CVE-2020-28015	New-line injection into spool header file (local)

CVE-2020-28012	Missing close-on-exec flag for privileged pipe
CVE-2020-28009	Integer overflow in get_stdinput()
Remote	
CVE-2020-28017	Integer overflow in receive_add_recipient()
CVE-2020-28020	Integer overflow in receive_msg()
CVE-2020-28023	Out-of-bounds read in smtp_setup_msg()
CVE-2020-28021	New-line injection into spool header file (remote)
CVE-2020-28022	Heap out-of-bounds read and write in extract_option()
CVE-2020-28026	Line truncation and injection in spool_read_header()
CVE-2020-28019	Failure to reset function pointer after BDAT error
CVE-2020-28024	Heap buffer underflow in smtp_ungetc()
CVE-2020-28018	Use-after-free in tls-openssl.c
CVE-2020-28025	Heap out-of-bounds read in pdkim_finish_bodyhash()

Patches, Mitigations, and Workarounds

HC3 recommends EXIM administrators update any EXIM platforms to version 4.94.2. It is highly advised to patch reported vulnerabilities to protect systems against possible exploits. Vulnerabilities should be triaged and prioritized for patching by healthcare organizations with special consideration to each vulnerability criticality category against the risk management posture of the enterprise. General information on the platform can be found at EXIM Internet Mailer and specific instructions on downloading the latest version can be found at their downloads site.

References

21Nails vulnerabilities impact 60% of the internet's email servers
https://therecord.media/21nails-vulnerabilities-impact-60-of-the-internets-email-servers/

21Nails: Multiple Critical Vulnerabilities in Exim Mail Server
https://blog.qualys.com/vulnerabilities-research/2021/05/04/21nails-multiple-vulnerabilities-in-exim-mail-server

Critical 21Nails Exim bugs expose millions of servers to attacks
https://www.bleepingcomputer.com/news/security/critical-21nails-exim-bugs-expose-millions-of-servers-to-attacks/

Mail (MX) Server Survey
http://www.securityspace.com/s_survey/data/man.202103/mxsurvey.html

Millions of Exim mail servers are currently under attack
https://securityaffairs.co/wordpress/87078/hacking/exim-servers-under-attacl.html

Qualys Security Advisory 21Nails: Multiple vulnerabilities in Exim
https://www.qualys.com/2021/05/04/21nails/21nails.txt

5 Open Source Security Risks You Should Know About
https://www.xfive.co/blog/5-open-source-security-risks/

CVE-2020-28007
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28007

CVE-2020-28008
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28008

CVE-2020-28014
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28014

CVE-2021-27216
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27216

CVE-2020-28011
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28011

CVE-2020-28010
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28010

CVE-2020-28013
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28013

CVE-2020-28016
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28016

CVE-2020-28015
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28015

CVE-2020-28012
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28012

CVE-2020-28009
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28009
CVE-2020-28017
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28017

CVE-2020-28020
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28020

CVE-2020-28023
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28023

CVE-2020-28021

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28021

CVE-2020-28022
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28022

CVE-2020-28026
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28026CVE-2020-28019

CVE-2020-28019
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28019

CVE-2020-28024
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28024

CVE-2020-28018
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28018

CVE-2020-28025
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28025