*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**TLP: WHITE**

https://www.cisa.gov/tlp

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

## DATE(S) ISSUED:

05/06/2021

## SUBJECT:

Multiple Vulnerabilities in Exim Could Allow for Remote Code Execution

## OVERVIEW:

Multiple vulnerabilities have been discovered in Exim, the most severe of which could allow for remote code execution. Exim is a mail transfer agent used to deploy mail servers on Unix-like systems. Successful exploitation of the most severe of these vulnerabilities will enable the attacker to perform command execution as root in the context of the mail server. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

## THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild. A proof of concept exists for various vulnerabilities mentioned within this advisory.

## SYSTEMS AFFECTED:

- Exim versions prior to 4.94.2

## RISK:

**Government:**

- Large and medium government entities: **High**
- Small government entities: **Medium**

**Businesses:**

- Large and medium business entities: **High**
- Small business entities: **Medium**

**Home users: Low**

## TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Exim , the most severe of which could allow for remote code execution. Details of these vulnerabilities are as follows:

- A security vulnerability exists due to a symlink error in Exim log directory. A local attacker can create a specially crafted symbolic link to a critical file on the system and overwrite it with privileges of the application. An attacker who obtained the privileges of the 'exim' user can exploit this local vulnerability to obtain full root privileges. (CVE-2020-28007)

- A privilege escalation vulnerability because it fails to properly impose security restrictions on the spool directory. A local attacker can exploit this issue to escalate privileges on the system. An attacker who obtained the privileges of the ‘exim’ user can exploit
- this local vulnerability to obtain full root privileges. (CVE-2020-28008)
- An local integer-overflow vulnerability. Specifically, this issue affects the 'get_stdinput()' function. (CVE-2020-28009)
- A local arbitrary code-execution vulnerability that occurs due to an out-of-bounds write error. Specifically, this issue affects the 'main()' function. An attacker can exploit this issue to execute arbitrary code within the context of the affected system. ( CVE-2020-28010)
- A heap-based buffer overflow vulnerability due to a boundary error. Specifically, this issue affects the 'queue_run()' function. A local attacker can exploit this issue execute arbitrary code with elevated privileges. An attacker who obtained the privileges of the ‘exim’ user can exploit this local vulnerability to obtain full root privileges. (CVE-2020-28011)
- A privilege-escalation vulnerability that exists due to missing close-on-exec flag for privileged pipe. A local attacker can exploit this issue to escalate privileges on the system. (CVE-2020-28012)
- A heap-based buffer overflow vulnerability due to a boundary error. Specifically, this issue affects the 'parse_fix_phrase()' function. A local attacker can exploit this issue execute arbitrary code with elevated privileges. (CVE-2020-28013)
- A security vulnerability because application uses PID files in an insecure manner. A local attacker who obtained the privileges of the ‘exim’ user can exploit this issue by predicting the name of the PID file and use it to escalate privileges on the system. (CVE-2020-28014)
- A security vulnerability that exists due to insufficient validation of user-supplied input when processing new line characters. A local attacker can inject a new line character into spool header file to execute arbitrary commands. (CVE-2020-28015)
- An arbitrary code-execution vulnerability that occurs due to an out-of-bounds write error. Specifically, this issue affects the 'parse_fix_phrase()' function. A local attacker can exploit this issue to execute arbitrary code within the context of the affected system. (CVE-2020-28016)
- An remote integer-overflow vulnerability. Specifically, this issue affects the 'get_stdinput()' function. (CVE-2020-28017)
- A remote Use-after-free vulnerability. Specifically in ‘tls-openssl.c’. An attacker can exploit this issue to execute arbitrary code within the context of the affected system as the ‘exim’ user. (CVE-2020-28018)
- A denial of service vulnerability exists, due to the failure to reset a function pointer after a BDAT error. (CVE-2020-28019)
- An remote integer-overflow vulnerability. Specifically, this issue affects the 'get_stdinput()' function as the ‘exim’ user. (CVE-2020-28020)
- A security vulnerability that exists due to insufficient validation of user-supplied input when processing new line characters. A remote attacker can inject a new line character into spool header file to execute arbitrary commands. (CVE-2020-28021)
- A remote arbitrary code-execution vulnerability that occurs due to an out-of-bounds read and write error. Specifically, this issue affects the 'main()' function. An attacker can exploit this issue to execute arbitrary code within the context of the affected system as the ‘exim’ user. (CVE-2020-28022)
- A remote security vulnerability exists that allows for an out-of-bounds read error. Specifically, this issue affects the smtp_setup_msg()' function. (CVE-2020-28023)

- A remote heap-based buffer underflow vulnerability due to a boundary error. Specifically, this issue affects the smtp_ungetc()' function. An attacker can exploit this issue execute arbitrary code with elevated privileges. (CVE-2020-28024)
- A remote security vulnerability occurs due to an out-of-bounds read error. Specifically, this issue affects the ' pdkim_finish_bodyhash()' function. A attacker can exploit this issue to disclose information. (CVE-2020-28025)
- A Line truncation and injection vulnerability exists that could allow an unauthenticated remote attacker to execute arbitrary commands as root (if DSN is enabled). Specifically this issue affects the 'spool_read_header()' function. (CVE-2020-28026)
- An Arbitrary file deletion vulnerability exists that could allow any local user to delete an arbitrary file as root. (CVE-2021-27216)

Successful exploitation of the most severe of these vulnerabilities will enable the attacker to perform command execution as root in the context of the mail server. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**RECOMMENDATIONS:**
The following actions should be taken:

- Apply appropriate patches provided by Exim to vulnerable systems immediately after appropriate testing
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Apply the principle of Least Privilege to all systems and services.
- Remind users not to open emails, download attachments, or follow links provided by unknown or untrusted sources.

**REFERENCES:**
**CVE:**
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28007
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28008
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28009
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28010
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28011
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28012
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28013
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28014
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28015
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28016
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28017
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28018
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28019
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28020
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28021
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28022
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28023
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28024
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28025
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28026
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27216

**EXIM:**
https://lists.exim.org/lurker/message/20210504.134007.ce022df3.en.html

**Qualys:**
https://www.qualys.com/2021/05/04/21nails/21nails.txt

**TLP: WHITE**
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.