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
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
08/08/2022

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:
Proof of concept code has been released for CVE-2022-37451 and CVE-2022-37452

SYSTEMS AFFECTED:

- Exim versions prior to 4.96

RISK:
Government:

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

Businesses:

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

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:

Tactic: *Execution* (TA0002):

Technique: *Native API* (T1106):

- A heap-based buffer overflow for the alias list in host_name_lookup in host.c when sender_host_name is set which could result in remote code execution. (CVE-2022-37452)
- An invalid free in pam_converse in auths/call_pam.c because store_free is not used after store_malloccould. (CVE-2022-37451)

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:
We recommend the following actions be taken:

- Apply appropriate patches provided by Exim to vulnerable systems, immediately after appropriate testing. (**M1051: Update Software**)
  - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
  - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
  - **Safeguard 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets:** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
- Block execution of code on a system through application control, and/or script blocking. (**M1038** : **Execution Prevention**)
  - **Safeguard 2.5 : Allowlist Authorized Software:** Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.
  - **Safeguard 2.6 : Allowlist Authorized Libraries:** Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.

Safeguard 2.7 : Allowlist Authorized Scripts: Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific

.ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.

REFERENCES:

Exim:https://www.exim.org/

CVE:https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37452

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37451

SecurityOnline:https://securityonline.info/cve-2022-37452-exim-heap-based-buffer-overflow-vulnerability/

GitHub/POC Code:https://github.com/ivd38/exim_overflow

https://github.com/ivd38/exim_invalid_free