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:
11/13/2021

SUBJECT:
A Vulnerability in Palo Alto PAN-OS Could Allow for Arbitrary Code Execution

OVERVIEW:
A vulnerability has been discovered in Palo Alto PAN-OS that could allow for arbitrary code execution. PAN-OS is the software that runs on all Palo Alto Network firewalls. Successful exploitation of this vulnerability could allow for arbitrary code execution with root privileges. 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 this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:
- Palo Alto PAN-OS versions prior to 10.1.3
- Palo Alto PAN-OS versions prior to 10.0.8
- Palo Alto PAN-OS versions prior to 9.1.11-h2
- Palo Alto PAN-OS versions prior to 8.1.20-h1

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:
A OS command injection vulnerability in the Simple Certificate Enrollment Protocol (SCEP) feature of PAN-OS could allow for arbitrary code execution. To successfully exploit, the attacker must have specific knowledge of the firewall configuration, and have network access to the GlobalProtect interfaces. When exploited, an attacker can run execute arbitrary code with root privileges.

Successful exploitation of this vulnerability could allow for arbitrary code execution with root privileges. 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:

- Restrict access to the GlobalProtect interface to authorized hosts only
- Apply appropriate patches or mitigations provided by Palo Alto to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Palo Alto:
https://security.paloaltonetworks.com/CVE-2021-3060

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3060