PTA Cyber Security Advisory No:084   **29-May-2020**

Name: Palo Alto Networks OS Injection Vulnerability in PAN-OS Management Server
   (CVE-2020-2014)

Threat Classification: Command Injection

Affected Systems: Affects the following Palo Alto Networks PAN-OS versions:

- All versions of PAN-OS 7.1 and 8.0

- PAN-OS 8.1 versions earlier than 8.1.14

- PAN-OS 9.0 versions earlier than 9.0.7

Summary:

Palo Alto Networks PAN-OS management server has an OS Command Injection vulnerability that allows the authenticated users to inject and execute arbitrary shell commands with root privileges.

Severity	HIGH
Attack Vector	Network
Privileges required	Low

For further details, please visit following official link:
https://security.paloaltonetworks.com/CVE-2020-2014

Recommendations:

- This issue is fixed in PAN-OS 8.1.14, 9.0.7, 9.1.0 and all later PAN-OS versions. Please visit following official link for the detailed information, documentation and remediation of the aforementioned vulnerability:
  https://docs.paloaltonetworks.com/pan-os.html

- Please also review the Best Practices for Securing Administrative Access in the PAN-OS technical documentation available at following official link:
  https://docs.paloaltonetworks.com/best-practices.html

- In all cases, ensure the availability of stable version, before upgrade, by the relevant vendor.

- In all cases, also ensure that devices to be upgraded to new release meet the requirements set by the vendor.

- Whenever required, access the system with minimal access rights and privileges.

- Use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.

- Only use licensed software and avoid download/use of cracked and pirated software.

- Designate a PoC from your security / Network team (if yet not designated), for seeking assistance and reporting security issues.

- In case of any incident, please report to this office.