Pakistan Telecom Authority Headquarter, Islamabad

PTA Cyber Security Advisory No: 074

31-March-2020

Name: Palo Alto Networks Shell Injection Vulnerability (CVE-2020-1980)

Threat Classification: Privilege Escalation

Affected Systems: Affects the following Palo Alto Networks product:

- PAN-OS 8.1 versions earlier than PAN-OS 8.1.13

Summary:

The PAN-OS CLI allows an authenticated user to escape the restricted shell and escalate privileges due to a shell command injection vulnerability. This security issue does not affect PAN-OS 7.1, PAN-OS 9.0, or later versions. This issue is fixed in PAN-OS 8.1.13, and all later versions.

Attack Severity	**HIGH**
Attack Type	Privilege Escalation
Privileges required	None

For further details, please visit following vendor official link:

https://security.paloaltonetworks.com/CVE-2020-1980

Recommendations:

- This security issue is mitigated by following the best practices for securing the PAN-OS management interface. Please visit following official website link for the remediation of the aforementioned vulnerability:

  https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/getting-started/best-practices-for-securing-administrative-access

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