## Pakistan Telecom Authority Headquarters, Islamabad

**PTA Cyber Security Advisory No:114** **25-11-2020**

**Name:** PaloAlto Networks (PAN) Authentication Bypass Vulnerability (CVE-2020-2050)

**Threat Classification:** Authentication Bypass

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

- PAN-OS 8.1 versions earlier than 8.1.17
- PAN-OS 9.0 versions earlier than 9.0.11
- PAN-OS 9.1 versions earlier than 9.1.5
- PAN-OS 10.0 versions earlier than 10.0.1

**Summary:**

An authentication bypass vulnerability exists in the GlobalProtect SSL VPN component of Palo Alto Networks software that allows an attacker to bypass all client certificate checks with an invalid certificate and gain access to restricted VPN network resources when the gateway or portal is configured to rely entirely on certificate-based authentication.

| **Severity** | HIGH |
|---|---|
| **Attack Vector** | Network |
| **Attack Complexity** | Low |
| **Privileges required** | None |

For further details, please visit following official link:
https://security.paloaltonetworks.com/CVE-2020-2050

## Recommendations:

- This vulnerability is fixed in PAN-OS 8.1.17, 9.0.11, 9.1.5, 10.0.1 and their all later 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 PaloAlto Networks best practices 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.