Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 247 **12-04-2024**

Name: Zero-Day Alert: Critical Palo Alto Networks PAN-OS Flaw Under Active Attack

Threat Classification: Vulnerability

Affected Software / Services:

- PAN-OS < 11.1.2-h3
- PAN-OS < 11.0.4-h1
- PAN-OS < 10.2.9-h1

Summary:

A critical flaw, tracked as CVE-2024-3400, has been discovered in Palo Alto Networks PAN-OS software used in GlobalProtect gateways. This flaw allows an unauthenticated attacker to execute arbitrary code with root privileges on the firewall, posing a severe risk to affected systems. The vulnerability affects specific PAN-OS versions and feature configurations. Palo Alto Networks is expected to release fixes on April 14, 2024.

Severity	**Critical**
Attack Vector	Command Injection / Network

Recommendations:

- Upgrade PAN-OS software to the latest versions provided by Palo Alto Networks, expected to be released on April 14, 2024, to mitigate the vulnerability.
- Customers with a Threat Prevention subscription should enable Threat ID 95187 to protect against potential exploitation of this vulnerability.
- Review configurations for both GlobalProtect gateway and device telemetry to ensure that only necessary features are enabled.
- Employ continuous monitoring and intrusion detection systems to detect any suspicious activity indicative of exploitation attempts.
- Restrict access to affected firewalls and apply the principle of least privilege to minimize the impact of potential attacks.
- Stay updated on security advisories and patches released by Palo Alto Networks to address emerging threats and vulnerabilities.
- In case of any incident, please report to this office, through PTA CERT Portal and email.