Security Advisory 2020-045

Vulnerabilities in Palo Alto PAN-OS

September 10, 2020 — v1.0

TLP:WHITE

History:

- 10/09/2020 — v1.0 – Initial publication

Summary

On 9th of September 2020, Palo Alto released several security advisories, updates, and workarounds to address security vulnerabilities including five high severity vulnerabilities and one critical one for PAN-OS [1-6]:

- CVE-2020-2040 PAN-OS: Buffer overflow when Captive Portal or Multi-Factor Authentication (MFA) is enabled - CVSS score 9.8 (critical)
- CVE-2020-2036 PAN-OS: Reflected Cross-Site Scripting (XSS) vulnerability in management web interface - CVSS score 8.8 (high)
- CVE-2020-2041 PAN-OS: Management web interface denial-of-service (DoS) - CVSS score 7.5 (high)
- CVE-2020-2037 PAN-OS: OS command injection vulnerability in the management web interface - CVSS score 7.2 (high)
- CVE-2020-2038 PAN-OS: OS command injection vulnerability in the management web interface - CVSS score 7.2 (high)
- CVE-2020-2042 PAN-OS: Buffer overflow in the management web interface - CVSS score 7.2 (high)

The critical vulnerability is exploitable only if Captive Portal or Multi-Factor Authentication (MFA) are enabled and does not impact GlobalProtect VPN or PAN-OS management web interfaces.

As of today, there is no known public proof-of-concept, however this type of vulnerabilities trigger high interest for different threat actors and proof-of-concept usually emerges quite quickly after the release of a patch. For this reason, it is highly recommended to patch the exposed PAN-OS devices as soon as possible.
Technical Details

CVE-2020-2040 (CVSS Score: Base 9.8)
A buffer overflow vulnerability in PAN-OS allows an unauthenticated attacker to disrupt system processes and potentially execute arbitrary code with root privileges by sending a malicious request to the Captive Portal or Multi-Factor Authentication interface. This issue does not impact the GlobalProtect VPN or the PAN-OS management web interfaces [4].

CVE-2020-2036 (CVSS Score: Base 8.8)
A reflected cross-site scripting (XSS) vulnerability exists in the PAN-OS management web interface. A remote attacker able to convince an administrator with an active authenticated session on the firewall management interface to click on a crafted link to that management web interface could potentially execute arbitrary JavaScript code in the administrator's browser and perform administrative actions [1].

CVE-2020-2041 (CVSS Score: Base 7.5)
An insecure configuration of the appweb daemon of Palo Alto Networks PAN-OS 8.1 allows a remote unauthenticated user to send a specifically crafted request to the device that causes the appweb service to crash. Repeated attempts to send this request result in denial of service to all PAN-OS services by restarting the device and putting it into maintenance mode [5].

CVE-2020-2037 (CVSS Score: Base 7.2)
An OS Command Injection vulnerability in the PAN-OS management interface that allows authenticated administrators to execute arbitrary OS commands with root privileges [2].

CVE-2020-2038 (CVSS Score: Base 7.2)
An OS Command Injection vulnerability in the PAN-OS management interface that allows authenticated administrators to execute arbitrary OS commands with root privileges [3].

CVE-2020-2042 (CVSS Score: Base 7.2)
A buffer overflow vulnerability in the PAN-OS management web interface allows authenticated administrators to disrupt system processes and potentially execute arbitrary code with root privileges [6].

Palo Alto Networks is not aware of any malicious attempts to exploit these vulnerabilities [1-6].

Products Affected

These vulnerabilities affect several versions of PAN-OS:

- PAN-OS 10.0;
- PAN-OS 9.1;
- PAN-OS 9.0;
- PAN-OS 8.1;

For specific affected versions, please refer to the Palo Alto security page [7].
Recommendations

CERT-EU recommends updating the vulnerable applications and systems or applying workarounds as soon as possible.

References

[1] https://security.paloaltonetworks.com/CVE-2020-2036