Health Sector Cybersecurity Coordination Center (HC3)
Sector Alert
June 30, 2020

CVE-2020-2021 PAN-OS: Authentication Bypass in SAML Authentication

Executive Summary

On June 29, 2020, Palo Alto Networks announced a vulnerability (CVE-2020-2021) affecting their PAN-OS firewall software. The vulnerability has a 10/10 CVSSv3 score which "means the vulnerability is both easy to exploit as it doesn't require advanced technical skills, and it's remotely exploitable via the internet, without requiring attackers to gain an initial foothold on the attacked device." Also on June 29, USCYBERCOM Cybersecurity Alert (@CNMF_CyberAlert) tweeted that they expected "Foreign APTs will likely attempt exploit soon."[1]

Analysis

According to Palo Alto:

In the case of GlobalProtect Gateways, GlobalProtect Portal, Clientless VPN, Captive Portal, and Prisma Access, an unauthenticated attacker with network access to the affected servers can gain access to protected resources if allowed by configured authentication and Security policies. There is no impact on the integrity and availability of the gateway, portal, or VPN server. An attacker cannot inspect or tamper with sessions of regular users. In the worst case, this is a critical severity vulnerability with a CVSS Base Score of 10.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N).

In the case of PAN-OS and Panorama web interfaces, this issue allows an unauthenticated attacker with network access to the PAN-OS or Panorama web interfaces to log in as an administrator and perform administrative actions. In the worst-case scenario, this is a critical severity vulnerability with a CVSS Base Score of 10.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). If the web interfaces are only accessible to a restricted management network, then the issue is lowered to a CVSS Base Score of 9.6 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

Alert

When Security Assertion Markup Language (SAML) authentication is enabled and the 'Validate Identity Provider Certificate' option is disabled (unchecked), improper verification of signatures in PAN-OS SAML authentication enables an unauthenticated network-based attacker to access protected resources. The attacker must have network access to the vulnerable server to exploit this vulnerability.

This issue affects PAN-OS 9.1 versions earlier than PAN-OS 9.1.3; PAN-OS 9.0 versions earlier than PAN-OS 9.0.9; PAN-OS 8.1 versions earlier than PAN-OS 8.1.15, and all versions of PAN-OS 8.0 (EOL). This issue does not affect PAN-OS 7.1.

This issue cannot be exploited if SAML is not used for authentication.

This issue cannot be exploited if the 'Validate Identity Provider Certificate' option is enabled (checked) in the SAML Identity Provider Server Profile.

Resources that can be protected by SAML-based single sign-on (SSO) authentication are:

[1] https://twitter.com/CNMF_CyberAlert/status/1277674547542659074

- *GlobalProtect Gateway,*
- *GlobalProtect Portal,*
- *GlobalProtect Clientless VPN,*
- *Authentication and Captive Portal,*
- *PAN-OS next-generation firewalls (PA-Series, VM-Series) and Panorama web interfaces,*
- *Prisma Access*

Patches, Mitigations & Workarounds:

- Updating PAN-OS versions to PAN-OS 8.1.15, PAN-OS 9.0.9, PAN-OS 9.1.3, or a later version.
- Using a different authentication method and disabling SAML authentication will completely mitigate the issue.
- Ensure that the 'Identity Provider Certificate' is configured and the identity provider (IdP) certificate is a certificate authority (CA) signed certificate, then ensure that the 'Validate Identity Provider Certificate' option is enabled in the SAML Identity Provider Server Profile.

References

- https://security.paloaltonetworks.com/CVE-2020-2021
- https://docs.paloaltonetworks.com/pan-os
- https://www.zdnet.com/article/us-cyber-command-says-foreign-hackers-will-most-likely-exploit-new-pan-os-security-bug/

Additional OSINT Resources

- Critical flaw opens Palo Alto Networks firewalls and VPN appliances to attack, patch ASAP!
- US Cyber Command highlights Palo Alto Networks security patch, citing foreign espionage