CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-056

Authentication-Bypass Vulnerability in PaloAlto GlobalProtect

November 13, 2020 — v1.0

TLP:WHITE

History:

- *13/11/2020 — v1.0 – Initial publication*

Summary

On 11th of November 2020, Palo Alto released a security advisory to address an authentication bypass vulnerability that exists in the GlobalProtect SSL VPN component of Palo Alto Networks PAN-OS software. The vulnerability allows an attacker to bypass all client certificate checks with an invalid certificate. A remote attacker can successfully authenticate as any user and gain access to restricted VPN network resources when the gateway or portal is configured to rely entirely on certificate-based authentication [1].

Technical Details

The vulnerability – CVE-2020-2050 – received the CVSS Base Score: 8.2 [2]. Impacted features that use SSL VPN with client certificate verification are:

- GlobalProtect Gateway
- GlobalProtect Portal
- GlobalProtect Clientless VPN

In configurations where client certificate verification is used in conjunction with other authentication methods, the protections added by the certificate check are ignored as a result of this issue.

This issue is only applicable to PAN-OS appliances using the GlobalProtect VPN, gateway, or portal configured to allow users to authenticate with client certificate authentication.

This issue can not be exploited if client certificate authentication is not in use.

Other forms of authentication are not impacted by this issue.

Affected Products

These vulnerabilities affect several versions of PAN-OS:

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

Recommendations

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

This issue is fixed in PAN-OS 8.1.17, PAN-OS 9.0.11, PAN-OS 9.1.5, PAN-OS 10.0.1, and all later PAN-OS versions.

Workarounds

Until PAN-OS software is upgraded to a fixed version, enabling signatures for Unique Threat ID 59884 on traffic destined for the GlobalProtect portal, gateway, or VPN will block attacks against CVE-2020-2050.

This issue can be mitigated by configuring GlobalProtect to require users to authenticate with their credentials. Other authentication methods are not impacted by this issue.

References

[1] https://security.paloaltonetworks.com/CVE-2020-2050

[2] https://cvssjs.github.io/#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

[3] https://cwe.mitre.org/data/definitions/285

[4] https://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-2050