CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-064

Critical Vulnerability in Palo Alto Security Appliances

November 11, 2021 — v1.0

TLP:WHITE

History:

- *11/11/2021 — v1.0 – Initial publication*

Summary

On November 10, Palo Alto issued an advisory about a critical vulnerability, named `CVE-2021-3064` and scored 9.8 out of 10, affecting some versions of its security appliances running PAN-OS [1].

Palo Alto is not aware of any malicious exploitation of the vulnerability although working exploits exist [2].

Technical details

The vulnerability `CVE-2021-3064` is due to a memory corruption vulnerability in Palo Alto Networks GlobalProtect portal and gateway interfaces. It could allow an unauthenticated remote attacker to execute arbitrary code with root privileges. The attacker must have network access to the GlobalProtect interface to exploit this issue [1].

Only PAN-OS firewall configurations with a GlobalProtect portal or gateway enabled are vulnerable.

Products affected

This issue impacts `PAN-OS 8.1` versions earlier than `PAN-OS 8.1.17` [1].

Recommendations

CERT-EU strongly recommends updating or upgrading affected versions of PAN-OS to a non-vulnerable version.

Mitigations

Palo Alto recommends enabling signatures for Unique Threat IDs `91820` and `91855` on traffic destined for GlobalProtect portal and gateway interfaces to block attacks against `CVE-2021-3064` [1]. No SSL decryption is required for detection.

References

[1] https://security.paloaltonetworks.com/CVE-2021-3064

[2] https://threatpost.com/massive-zero-day-hole-found-in-palo-alto-security-appliances/176170/