Hive Pro

THREAT ADVISORY

A zero-day vulnerability has been discovered in PAN's GlobalProtect firewall

TA202148

Threat Level AMBER

Publish Date – Nov 14, 2021

Palo Alto Networks (PAN) released an update on November 10, 2021, that patched CVE-2021-3064, which was discovered and disclosed by Randori. This vulnerability affects PAN firewalls that use the GlobalProtect Portal VPN, and it allows for unauthenticated remote code execution on susceptible product installations. The vulnerability affects all versions of PAN-OS 8.1 prior to 8.1.17, and Randori has discovered over 10,000 vulnerable instances on internet-facing assets.

The CVE-2021-3064 vulnerability is a buffer overflow that occurs while parsing user-supplied information into a fixed-length position on the stack. Without using an HTTP smuggling approach, the troublesome code is not accessible from the outside world. An unauthenticated network-based attacker can disrupt system operations and potentially execute arbitrary code with root privileges by exploiting a memory corruption vulnerability in Palo Alto Networks GlobalProtect portal and gateway interfaces. To exploit this vulnerability, the attacker must have network access to the GlobalProtect interface.

An attacker must have network access to the device on the GlobalProtect service port(default port 443) in order to exploit this issue. This port is frequently accessible over the Internet since the impacted product is a VPN portal. Exploitation is challenging but not impossible on devices that have ASLR enabled. Due to the lack of ASLR on virtualized devices, exploitation is considerably easier.

Organizations can mitigate this vulnerability as follows:

1. A patch issued by the PAN should be used.(Link below)
2. PAN has also made Threat Prevention signatures 91820 and 91855 accessible for use by organizations to avoid exploitation until a software upgrade is scheduled.
3. Organizations that do not use the PAN firewall's VPN features should immediately disable GlobalProtect.

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-3064	Palo Alto PAN-OS versions 8.1.0, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.1.5, 8.1.6, 8.1.7, 8.1.8, 8.1.9, 8.1.10, 8.1.11, 8.1.12, 8.1.13, 8.1.14, 8.1.15, 8.1.16	cpe:2.3:a:palo_alto:pan-os:8.1.0:*:*:*:*:*:*:*, cpe:2.3:a:palo_alto:pan-os:8.1.1:*:*:*:*:*:*:*, cpe:2.3:a:palo_alto:pan-os:8.1.2:*:*:*:*:*:*:*, cpe:2.3:a:palo_alto:pan-os:8.1.3:*:*:*:*:*:*:*, cpe:2.3:a:palo_alto:pan-os:8.1.4:*:*:*:*:*:*:*, cpe:2.3:a:palo_alto:pan-os:8.1.5:*:*:*:*:*:*:*, cpe:2.3:a:palo_alto:pan-os:8.1.6:*:*:*:*:*:*:*, cpe:2.3:a:palo_alto:pan-os:8.1.7:*:*:*:*:*:*:*, cpe:2.3:a:palo_alto:pan-os:8.1.8:*:*:*:*:*:*:*, cpe:2.3:a:palo_alto:pan-os:8.1.9:*:*:*:*:*:*:*, cpe:2.3:a:palo_alto:pan-os:8.1.10:*:*:*:*:*:*:*, cpe:2.3:a:palo_alto:pan-os:8.1.11:*:*:*:*:*:*:*, cpe:2.3:a:palo_alto:pan-os:8.1.12:*:*:*:*:*:*:*, cpe:2.3:a:palo_alto:pan-os:8.1.13:*:*:*:*:*:*:*, cpe:2.3:a:palo_alto:pan-os:8.1.14:*:*:*:*:*:*:*, cpe:2.3:a:palo_alto:pan-os:8.1.15:*:*:*:*:*:*:*, cpe:2.3:a:palo_alto:pan-os:8.1.16:*:*:*:*:*:*:*	PAN-OS: Memory Corruption Vulnerability in GlobalProtect Portal and Gateway Interfaces	CWE-121

Patch Link

https://security.paloaltonetworks.com/CVE-2021-3064

References

https://www.randori.com/blog/cve-2021-3064/
https://threatpost.com/massive-zero-day-hole-found-in-palo-alto-security-appliances/176170/