# New PAN-OS DDoS flaw exploited in attacks

Severity: High

Date: 16th Aug 2022

## Description

Palo Alto Networks has issued a security advisory warning of an actively exploited high-severity vulnerability impacting PAN-OS, the operating system used by the company's networking hardware products.

## How It Works

The issue, tracked as CVE-2022-0028 (CVSS v3 – 8.6), is an URL filtering policy misconfiguration that could allow an unauthenticated, remote attacker to carry out amplified TCP denial-of-service (DoS) attacks.

PAN-OS versions vulnerable to this vulnerability are:

- PAN-OS prior to 10.2.2-h2 (patch ETA: next week)
- PAN-OS prior to 10.1.6-h6 (patch available)
- PAN-OS prior to 10.0.11-h1 (patch ETA: next week)
- PAN-OS prior to 9.1.14-h4 (patch ETA: next week)
- PAN-OS prior to 9.0.16-h3 (patch ETA: next week)
- PAN-OS prior to 8.1.23-h1 (patch ETA: next week)

Using the vulnerability, a hacker could enlist a Palo Alto Networks PAN-OS device for DDoS attacks, obfuscating the original IP of the threat actor and making remediation more challenging. Threat actors could use these attacks for various malicious behavior, such as extortion or to disrupt a company's business operations.

However, the vendor states that CVE-2022-0028 does not impact the products' confidentiality, integrity, or availability, so the attack potential is limited to DoS.

# Vulnerability Prerequisites

The vulnerable PAN-OS versions run inside PA-Series, VM-Series, and CN-Series devices, but the exploit only works when the following three conditions apply:

- The security policy on the firewall that allows traffic to pass from Zone A to Zone B includes a URL filtering profile with one or more blocked categories.
- Packet-based attack protection is not enabled in a Zone Protection profile for Zone A, including both (Packet Based Attack Protection > TCP Drop > TCP Syn With Data) and (Packet Based Attack Protection > TCP Drop > Strip TCP Options > TCP Fast Open).
- Flood protection through SYN cookies is not enabled in a Zone Protection profile for Zone A (Flood Protection > SYN > Action > SYN Cookie) with an activation threshold of 0 connections.

"The URL filtering policies are intended to be triggered when a user inside a protected network request to visit dangerous or disallowed sites on the Internet in traffic destined to the Internet."

"Such URL filtering is not meant to be used in the other direction for traffic coming from the Internet to the protected network."

"URL filtering in that direction offers no benefits. Hence any firewall configuration that is doing this is likely unintentional and considered a misconfiguration."

While a misconfiguration is required to remotely use a PAN-OS device to perform RDoS attacks, Palo Alto Networks is fixing the bug to prevent it from being abused both remotely and internally.

Since a security update isn't available for most PAN-OS version branches, system administrators are advised to ensure that at least one of the three prerequisites isn't met.

# Reference Links

- https://www.bleepingcomputer.com/news/security/palo-alto-networks-new-pan-os-ddos-flaw-exploited-in-attacks/
- https://security.paloaltonetworks.com/CVE-2022-0028