

**THREAT ADVISORY**



**VULNERABILITY  
REPORT**

**Denial-of-service vulnerability in PAN-OS  
exploited-in-the-wild**

Date of Publication

August 23, 2022

Admiralty Code

A1


TA Number

TA2022179

# Summary

The URL filtering policy misconfiguration in PAN-OS leads to a vulnerability that could allow an unauthenticated remote attacker to conduct distributed denial-of-service(DDoS) attacks. This vulnerability has been tracked as CVE-2022-0028.

## ⚙️ CVEs Table

CVE	NAME	PATCH
CVE-2022-0028	PAN-OS: Reflected Amplification Denial-of-Service (DoS) Vulnerability in URL Filtering	

## 🔗 Potential MITRE ATT&CK TTPs

<b>TA0040</b> Impact	<b>T1498</b> Network Denial of Service	<b>T1498.002</b> Network Denial of Service: Reflection Amplification	<b>TA0005</b> Defense Evasion
<b>T1027</b> Obfuscated Files or Information			

# Technical Details

## #1

It is only possible to exploit these vulnerable versions of PAN-OS if the following three conditions are met:

1. 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.
2. 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).
3. 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.

## #2

By exploiting the vulnerability, an attacker could obfuscate their original IP address and make remediation more difficult. Attackers could use these attacks for extortion or disrupt a company's business operations.

## #3

Though exploitation of this issue does not impact the confidentiality, integrity, or availability of your firewall or appliance, the resulting denial-of-service (DoS) attack can potentially result in a loss of availability for the attacker-specified target if that target lacks sufficient DoS protection.

## Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-0028	Palo Alto PAN-OS: 8.1 - 8.1.23, 9.0 - 9.0.16-hf, 9.1 - 9.1.14-h1, 10.0.0 - 10.0.11, 10.1.0 - 10.1.6, 10.2.0 - 10.2.2	cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*	CWE-406

## Patch Details

Upgrade to Palo Alto PAN-OS versions above 10.2.2-h2, 10.1.6-h6, 10.0.11-h1, 9.1.14-h4, 9.0.16-h3, 8.1.23-h1

## References

<https://security.paloaltonetworks.com/CVE-2022-0028>

# What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.



At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

**August 23, 2022 • 6:15 AM**

© 2022 All Rights are Reserved by HivePro



More at [www.hivepro.com](https://www.hivepro.com)