# Advisory Alert

**Alert Number:** **AAA20241227** **Date:** **December 27, 2024**

**Document Classification Level** : Public Circulation Permitted | Public

**Information Classification Level** : TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Palo Alto** | **High** | Denial of Service Vulnerability |

## Description

| | |
|---|---|
| Affected Product | **Palo Alto** |
| Severity | **High** |
| Affected Vulnerability | Denial of Service Vulnerability (CVE-2024-3393) |
| Description | Palo Alto has released security updates addressing a Denial of Service Vulnerability that exists in DNS Security feature of Palo Alto Networks PAN-OS software which allows an unauthenticated attacker to send a malicious packet through the data plane of the firewall that reboots the firewall. Repeated attempts to trigger this condition will cause the firewall to enter maintenance mode.<br>Palo Alto advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | PAN-OS 11.2 - versions prior to 11.2.3<br>PAN-OS 11.1 - versions prior to 11.1.5<br>PAN-OS 10.2:<br>• Versions 10.2.8 and later<br>• 10.2.10 versions prior to 10.2.10-h12<br>• 10.2.13 versions prior to 10.2.13-h2<br>PAN-OS 10.1 - versions 10.1.14 and up to 10.1.14-h8<br>Prisma Access on PAN-OS - versions 10.2.8 and up to 11.2.3 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://security.paloaltonetworks.com/CVE-2024-3393 |

### Disclaimer

**The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.**