PAN-OS: Heap-Based Buffer Overflow in DNS Proxy and DNS Server Allows Unauthenticated Remote Code Execution

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-0264
State	PUBLISHED
Assigner	palo_alto
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-13 18:16:14 UTC
Updated	2026-05-13 18:17:47 UTC
Description	A buffer overflow vulnerability in the DNS proxy and DNS Server features of Palo Alto Networks PAN-OS® Software allows

Risk And Classification

Primary CVSS: v4.0 7.2 HIGH from psirt@paloaltonetworks.com

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:Y/R:U/V:C/RE:H/U:Red

Problem Types: CWE-122 | CWE-122 CWE-122 Heap-based Buffer Overflow

Version	Source	Type	Score	Severity	Vector
4.0	psirt@paloaltonetworks.com	Secondary	7.2	HIGH	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/S
4.0	CNA	CVSS	7.2	HIGH	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/S
4.0	CNA	CVSS	6.6	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:Y/R:U/V:C/RE:H/U:Red

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Palo Alto Networks	Cloud NGFW	unaffected All custom
CNA	Palo Alto Networks	PAN-OS	affected 12.1.0 12.1.7, 12.1.4-h5 custom
CNA	Palo Alto Networks	PAN-OS	affected 11.2.0 11.2.12, 11.2.10-h6, 11.2.7-h13, 11.2.4-h17 custom
CNA	Palo Alto Networks	PAN-OS	affected 11.1.0 11.1.15, 11.1.13-h5, 11.1.10-h25, 11.1.7-h6, 11.1.6-h32, 11.1.4-h33 custom
CNA	Palo Alto Networks	PAN-OS	affected 10.2.0 10.2.18-h6, 10.2.16-h7, 10.2.13-h21, 10.2.10-h36, 10.2.7-h34 custom
CNA	Palo Alto Networks	Prisma Access	unaffected All custom

References

Reference	Source	Link	Tags
security.paloaltonetworks.com/CVE-2026-0264	psirt@paloaltonetworks.com	security.paloaltonetworks.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Palo Alto Networks thanks an external reporter and our internal security research teams for discovering and reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-05-13T16:00:00.000Z	Initial Publication.

Solutions

CNA: VERSION MINOR VERSION SUGGESTED SOLUTION Cloud NGFW No action needed PAN-OS 12.1 12.1.5 through 12.1.6 Upgrade to 12.1.7 or later. 12.1.2 through 12.1.4-h* Upgrade to 12.1.4-h5 or 12.1.7 or later. PAN-OS 11.2 11.2.11 or later Upgrade to 11.2.12 or later. 11.2.8 through 11.2.10-h* Upgrade to 11.2.10-h6 or 11.2.12 or later. 11.2.5 through 11.2.7-h* Upgrade to 11.2.7-h13 or 11.2.10 or later. 11.2.0 through 11.2.4-h* Upgrade to 11.2.4-h17 or 11.2.7 or later. PAN-OS 11.1 11.1.14 or later Upgrade to 11.1.15 or later. 11.1.11 through 11.1.13-h* Upgrade to 11.1.13-h5 or 11.1.15 or later. 11.1.8 through 11.1.10-h* Upgrade to 11.1.10-h25 or 11.1.15 or later. 11.1.7 through 11.1.7-h* Upgrade to 11.1.7-h6 or 11.1.15 or later. 11.1.5 through 11.1.6-h* Upgrade to 11.1.6-h32 or 11.1.15 or later. 11.1.0 through 11.1.4-h* Upgrade to 11.1.4-h33 or 11.1.15 or later. PAN-OS 10.2 10.2.17 through 10.2.18-h* Upgrade to 10.2.18-h6 or later. 10.2.14 through 10.2.16-h* Upgrade to 10.2.16-h7 or 10.2.18-h6 or later. 10.2.11 through 10.2.13-h* Upgrade to 10.2.13-h21 or 10.2.18-h6 or later. 10.2.8 through 10.2.10-h* Upgrade to 10.2.10-h36 or 10.2.18-h6 or later. 10.2.0 through 10.2.7-h* Upgrade to 10.2.7-h34 or 10.2.18-h6 or later. Prisma Access No action needed. All older unsupported PAN-OS versions Upgrade to a supported fixed version.

Workarounds

CNA: Customers can mitigate the risk of this issue by taking either of the following actions: Action 1: * Disassociate DNS Proxy from externally accessible interfaces in order to reduce your attack surface; AND * Configure DNS server with a RFC1918 or a public trusted IP address. OR Action 2: * Disable the DNS Proxy feature (Network > DNS Proxy) if it is not being used; AND * Configure DNS server with a RFC1918 or a public trusted IP address. Customers with a Threat Prevention subscription can block attacks for this vulnerability by enabling Threat ID 510027 from Applications and Threats content version 9100-10044 and later.

Exploits

CNA: Palo Alto Networks is not aware of any malicious exploitation of this issue.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**