WildFire WF-500 and WF-500-B: Arbitrary File Read and Delete Vulnerability in WildFire Appliance (WF-500, WF-500-B)

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

Summary

CVE	CVE-2026-0259
State	PUBLISHED
Assigner	palo_alto
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-13 19:17:01 UTC
Updated	2026-05-14 16:21:23 UTC
Description	An arbitrary File Read and Delete Vulnerability in Palo Alto Networks WildFire® WF-500 and WF-500-B appliances enables

Risk And Classification

Primary CVSS: v4.0 5 MEDIUM from psirt@paloaltonetworks.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/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:M/U:Amber

EPSS: 0.000500000 probability, percentile 0.155790000 (date 2026-05-17)

Problem Types: CWE-73 | CWE-73 CWE-73 External Control of File Name or Path

Version	Source	Type	Score	Severity	Vector
4.0	psirt@paloaltonetworks.com	Secondary	5	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/S
4.0	CNA	CVSS	5	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/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:M/U:Amber

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Palo Alto Networks	WildFire WF-500 And WF-500-B	affected 12.1.0 12.1.7, 12.1.4-h5 custom
CNA	Palo Alto Networks	WildFire WF-500 And WF-500-B	affected 11.2.0 11.2.11,11.2.7-h7 custom
CNA	Palo Alto Networks	WildFire WF-500 And WF-500-B	affected 11.1.0 11.1.13,11.1.10-h8 custom
CNA	Palo Alto Networks	WildFire WF-500 And WF-500-B	affected 10.2.0 10.2.18-h6, 10.2.16-h7, 10.2.13-h21, 10.2.10-h36, 10.2.7-h

References

Reference	Source	Link	Tags
security.paloaltonetworks.com/CVE-2026-0259	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 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 RANGE SUGGESTED SOLUTION WildFire WF-500 and WF-500-B 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. WildFire WF-500 and WF-500-B 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 11.2.12 or later. 11.2.0 through 11.2.4-h* Upgrade to 11.2.4-h17 or 11.2.12 or later. WildFire WF-500 and WF-500-B 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. WildFire WF-500 and WF-500-B 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. WildFire WF-500 and WF-500-B 10.1 All (EoL) No fix planned. Upgrade to a supported version.

Workarounds

CNA: For airgapped deployments, we strongly recommend that you secure WildFire 500 appliances by restricting access to only trusted internal IP addresses. Customers with a Threat Prevention subscription can block attacks for this vulnerability by enabling Threat ID 510010 (Applications and Threats content version 9100-10044 and later). Please note that this Threat ID requires SSL Decryption.

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.