



USER INTERACTION  
None

## CVE-2024-3400

Disclosure Date

CVE-2024-3400

⚠ Exploited in the wild

Reported by **cbeek-r7**  
[View Source Details](#)

[Report As Exploited in the Wild](#)

### Quick Cookie Notification

This site uses cookies for anonymized analytics to improve the site.

Rapid7 will never sell the data collected on this site.

[I AGREE, LET'S GO!](#)

[View our Cookie Policy for full details](#)

#### Watch This Topic

Watch this topic to be notified when new information, assessments, and comments are added

**MITRE ATT&CK**  
tag

[Log in to add MITRE ATT&CK](#)

**Metasploit Module**  
[exploit/linux/http/panos\\_telemetry\\_c...](#)

Add MITRE ATT&CK tactics and techniques that apply to this CVE.

#### Execution

TECHNIQUES

VALIDATION ⓘ

Command and Scripting  
Interpreter: Unix Shell

VALIDATED

#### Initial Access

TECHNIQUES

VALIDATION ⓘ

Exploit Public-Facing  
Application

VALIDATED

CISA KEV Listed

Common in enterprise

Easy to weaponize

Gives privileged access

Unauthenticated

Vulnerable in default configuration



## CVE-2024-3400

15

of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall.

Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability.



Ratings & Analysis

Vulnerability Details

**RAPID7** Analysis

### Quick Cookie Notification ×

This site uses cookies for anonymized analytics to improve the site.

Rapid7 will never sell the data collected on this site.

---

[View our Cookie Policy](#) for full details



ATTACKER VALUE  
**VERY HIGH**

**CVE-2024-3400**

15



## Quick Cookie Notification ×

This site uses cookies for anonymized analytics to improve the site.

Rapid7 will never sell the data collected on this site.

---

[View our Cookie Policy](#) for full details

[Terms of Use](#)

[Code of Conduct](#)

[FAQ](#)

[Changelog](#)

[Privacy Policy](#)

[Contact](#)

[API](#)

A Rapid7 Project

