



PAN-OS GlobalProtect Command Injection Vulnerability

An actively exploited critical vulnerability in the PAN-OS Global Protect

<https://security.paloaltonetworks.com/CVE-2024-3400>

CVEs: [CVE-2024-3400](#)

The attack on PAN-OS GlobalProtect devices identified as CVE-2024-3400 allows a malicious actor to remotely exploit an unauthenticated command injection vulnerability that leads to remote code execution. Once established, the attacker can further collect configurations, deliver malware payloads and move laterally into the network.

Background

The GlobalProtect Gateway provides security solution for roaming users by extending the same next-generation firewall-based policies.

Latest Developments

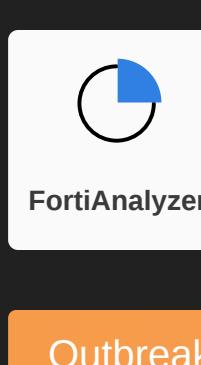
The FortiGuard is continuously monitoring and investigating the attack to increase protection coverages and reduce the attack surface.

- September 25, 2025: RedNovember (which overlaps with Storm-2077) targeted perimeter appliances of high-profile organizations globally.
<https://www.recordedfuture.com/research/rednovember-targets-government-defense-and-technology-organizations>
- September 02, 2025: People's Republic of China (PRC) state-sponsored cyber threat actors are targeting networks globally.
https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a?utm_source=SaltTyphoon&utm_medium=GovDelivery
- March 05, 2025: In March 2024, Silk Typhoon used a zero-day exploit for CVE-2024-3400 in GlobalProtect Gateway on Palo Alto Networks firewalls to compromise multiple organizations.
<https://www.microsoft.com/en-us/security/blog/2025/03/05/silk-typhoon-targeting-it-supply-chain/>
- April 15, 2024: FortiGuard released an IPS signature to detect and block exploitation attempts targeting edge devices. Also, FortiGuard published an Outbreak walkthrough video.
<https://www.fortiguard.com/encyclopedia/ips/55555>
- April 12, 2024: FortiGuard published this Outbreak Alert report.
- April 12, 2024: FortiGuard issued a Threat Signal.
<https://www.fortiguard.com/threat-signal-report/5423/pan-os-critical-flaw-in-globalprotect-gateway-cve-2024-3400>
- April 11, 2024: Palo Alto Networks released a security advisory on their GlobalProtect.
<https://security.paloaltonetworks.com/CVE-2024-3400>
- April 10, 2024: Volexity identified zero-day exploitation of a vulnerability found within the GlobalProtect.
<https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/>

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

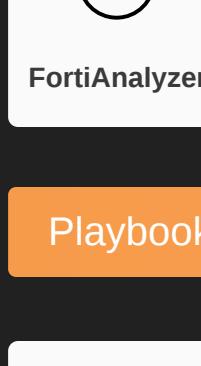
Lure



FortiDeceptor

DB 20240423

Decoy VM

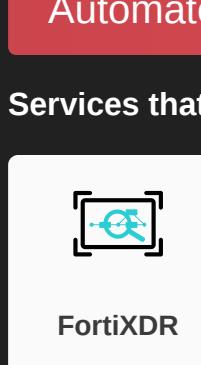


FortiDeceptor

DB 20240423

AV

Detects known malware related to the Outbreak

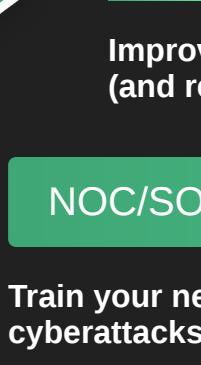


FortiClient

DB 92.03310

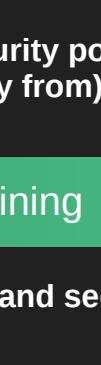
IPS

Detects and blocks attack attempts leveraging the vulnerability



FortiADC

DB 27.768



FortiGate

DB 27.768



FortiNDR

DB 27.768



FortiProxy

DB 27.768



FortiSASE

DB 27.768

Web App Security

Detects and blocks attack attempts leveraging the vulnerability



FortiADC

DB 1.00051



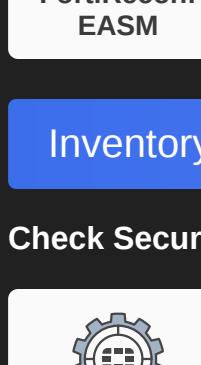
FortiWeb

DB 0.00375

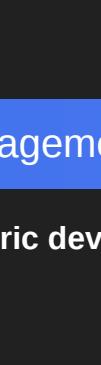
DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

IOC



FortiAnalyzer



FortiSOCaaS



FortiSIEM



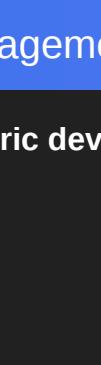
FortiSOAR

Outbreak Detection

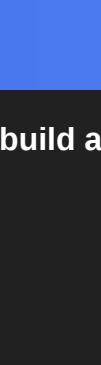


FortiAnalyzer

DB 2.00043



FortiSIEM



FortiSOAR

v7.4+

Threat Hunting

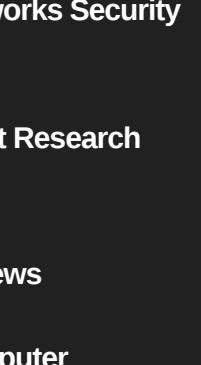


FortiAnalyzer

FortiSIEM

v7.4+

Playbook



FortiSOAR

v7.4+

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

FortiSOAR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

FortiSOAR

Response

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

NSE Training

Response

DB 607

End-User Training

Raise security awareness of your employees that are continuously being targeted by phishing, drive-by download

Awareness & Training

DB 11391

Playbook

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the

NSE Training

Response

DB 607

End-User Training

Raise security awareness of your employees that are continuously being targeted by phishing, drive-by download

Awareness & Training

DB 11391

Playbook

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

Security Rating

FortiDAST

DB 27.768

Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.

FortiRecon

v7.4+

Inventory Management

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

IoT and OT Detection

DB 27.768

Business Reputation

Know attackers next move to protect against your business branding.

FortiRecon

v7.4+

Additional Resources

Palo Alto Networks Security Advisories

<https://security.paloaltonetworks.com/CVE-2024-3400>

Volexity Threat Research

<https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/>

The Hacker News

<https://thehackernews.com/2024/04/zero-day-alert-critical-vulnerability-in-globalprotect-cve-2024-3400/>

Bleeping Computer

<https://www.bleepingcomputer.com/news/security/palo-alto-networks-warns-of-pan-os-firewall-zero-day-used-in-attacks/>

Microsoft Blog

<https://techcommunity.microsoft.com/microsoft-defender-vulnerability/defender-support-for-cve-2024-3400-affecting-palo-alto-networks/ba/411391>

Learn more about FortiGuard Outbreak Alerts

