FORTINET

OUTBREAK ALERTS

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 and internally.

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.

Apr 25, 2024: The FortiGuard Labs noted a significant increase in the detection of IPS signatures through FortiGuard telemetry, blocking attacks on over 10,000+ unique IPS devices targeting the PAN-OS vulnerability (CVE-2024-3400).

Apr 19, 2024: Palo Alto released more information on CVE-2024-3400 and how it was attacked.
https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/

Apr 15, 2024: FortiGuard released an IPS signature to detect and block exploitation attempts targeting edge devices.
https://www.fortiguard.com/encyclopedia/ips/55555

Apr 12, 2024: FortiGuard published this Outbreak Alert report.

Apr 12, 2024: FortiGuard issued a Threat Signal.
https://www.fortiguard.com/threat-signal-report/5423/

Apr 11, 2024: Palo Alto Networks released a security advisory on their GlobalProtect.
https://security.paloaltonetworks.com/CVE-2024-3400

Apr 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:

Reconnaissance

Lure

- FortiDeceptor

Decoy VM

- FortiDeceptor

Weaponization

Delivery

AV

Detects and blocks known malware related to the PAN-OS GlobalProtect Attack (CVE-2024-3400)

FortiGate	FortiWeb	FortiClient	FortiSASE	FortiMail	FortiCASB	FortiCWP
DB 92.03313	DB 92.03313	DB 92.03313	DB 92.03313	DB 92.03313	DB 92.03313	DB 92.03313

FortiADC	FortiProxy
DB 92.03313	DB 92.03313

AV (Pre-filter)

Detects and blocks known malware related to the PAN-OS GlobalProtect Attack (CVE-2024-3400)

FortiEDR	FortiSandbox	FortiNDR
DB 92.03313	DB 92.03313	DB 92.03313

Exploitation

IPS

Detects and blocks exploitation attempts targeting the PAN-OS Global Protect vulnerability (CVE-2024-3400)

FortiGate	FortiSASE	FortiNDR	FortiADC	FortiProxy
DB 27.768	DB 27.768	DB 27.768	DB 27.768	DB 27.768

Installation

C2

Action

DETECT

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

Outbreak Detection

- FortiAnalyzer
  DB 2.00043

Threat Hunting

- FortiAnalyzer

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

Assisted Response Services

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

- Incident Response
- FortiRecon: ACI

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 cyberattacks.

- NSE Training
- Response Readiness

End-User Training

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download and other forms of cyberattacks.

- Security Awareness & Training

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

Inventory Management

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

- IoT and OT Detection

Business Reputation

Know attackers next move to protect against your business branding.

- FortiRecon: EASM
- FortiRecon: BP

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-palo-alto.html
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/t5/microsoft-defender-vulnerability/defender-support-for-cve-2024-3400-affecting-palo-alto-networks/ba-p/4113917

Learn more about FortiGuard Outbreak Alerts