Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Zero-Day Flaw in Palo Alto Networks PAN-OS Patched After Active Exploitation

Date of Publication	Admiralty Code	TA Number
April 15, 2024	A1	TA2024146

Summary

First Seen: March 26, 2024
Affected Platform: Palo Alto Networks PAN-OS
Malware: UPSTYLE
Threat Actor: UTA0218
Impact: CVE-2024-3400 is a critical vulnerability in Palo Alto Networks PAN-OS software's GlobalProtect feature, allowing unauthenticated attackers to execute code with root privileges, potentially leading to full device control. Public exploit code exists. Patch and mitigation available, apply immediately.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-3400	Palo Alto Networks PAN-OS Command Injection Vulnerability	Palo Alto Networks PAN-OS	✓	✓	✓

Vulnerability Details

#1 CVE-2024-3400 is a critical unauthenticated remote code execution (RCE) vulnerability discovered in Palo Alto Networks PAN-OS software, specifically within the GlobalProtect feature. This vulnerability allows attackers to execute arbitrary code with root privileges on the firewall, potentially granting them full control over the device without requiring any credentials.

#2 The exploit associated with this vulnerability has been attributed to a threat actor known as UTA0218, while Palo Alto Networks refers to the campaign as “Operation MidnightEclipse”. Upon successful exploitation, the attacker could compromise firewall devices, establish a reverse shell, and download additional tools. The attacker's primary objective was to extract configuration data and move laterally within victim organizations, aiming to access sensitive credentials.

#3

In their efforts, the attacker attempted to deploy a Python-based backdoor named UPSTYLE. Post-exploitation activities included lateral movement and data theft. The attacker's infrastructure utilized a combination of command-and-control servers and anonymized sources, including compromised AWS buckets and VPNs. The sophistication of the attacker's methods suggests potential state-backed involvement.

#4

To address this vulnerability, Palo Alto Networks has released hotfixes 11.1.2-h3, 11.0.4-h1, and 10.2.9-h1 for PAN-OS versions 11.1, 11.0, and 10.2 with configurations for GlobalProtect gateway or GlobalProtect portal (or both) and device telemetry enabled. It's important to note that cloud firewalls, Panorama appliances, and Prisma Access are not affected by this vulnerability. Organizations are strongly advised to promptly apply these hotfixes and implement robust detection measures to mitigate the risk of exploitation.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-3400	Palo Alto PAN-OS: 10.2 < 10.2.9-h1 Palo Alto PAN-OS: 11.0 <11.0.4-h1 Palo Alto PAN-OS: 11.1 < 11.1.2-h3 11.1.2-h2	cpe:2.3:a:paloaltonetworks:pan-os:*:*:*:*:*:*:*	CWE-77

Recommendations

Upgrade PAN-OS Versions: Ensure that your organization upgrades to the fixed PAN-OS versions (10.2.9-h1, 11.0.4-h1, 11.1.2-h3, or later versions) as soon as possible. Regularly check for updates and apply them promptly to mitigate security risks.

Disable Unnecessary Features: Disable any unnecessary features or services within the GlobalProtect firewall device configuration. This can help reduce the attack surface and limit the potential impact of exploitation.

Implement Network Segmentation: Implement network segmentation to isolate critical systems and sensitive data from potentially compromised devices. By segmenting the network, organizations can contain and mitigate the impact of a successful compromise.

Enhance Access Controls: Review and strengthen access controls for firewall management interfaces and administrative accounts. Implement strong password policies, multi-factor authentication (MFA), and regularly audit user access rights to minimize the risk of unauthorized access.

Vulnerability Scanning: Conduct regular vulnerability scans on your network to identify any potential weaknesses or unpatched software. This proactive approach allows you to address security issues promptly before they can be exploited by attackers.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0007** Discovery
TA0006 Credential Access	**TA0009** Collection	**TA0011** Command and Control	**TA0042** Resource Development
T1588 Obtain Capabilities	**T1203** Exploitation for Client Execution	**T1588.005** Exploits	**T1588.006** Vulnerabilities
T1059.006 Python	**T1059** Command and Scripting Interpreter	**T1071.001** Web Protocols	**T1071** Application Layer Protocol
T1003.003 NTDS	**T1003** OS Credential Dumping	**T1584** Compromise Infrastructure	**T1557** Adversary-in-the-Middle
T1005 Data from Local System	**T1190** Exploit Public-Facing Application	**T1555** Credentials from Password Stores	**T1083** File and Directory Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	161fd76c83e557269bee39a57baa2ccbbac679f59d9adff1e1b73b0f4bb277a6, 35a5f8ac03b0e3865b3177892420cb34233c55240f452f00f9004e274a85703c, 3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac, 448fbd7b3389fe2aa421de224d065cea7064de0869a036610e5363c931df5b7c, 755f5b8bd67d226f24329dc960f59e11cb5735b930b4ed30b2df77572efb32e8, 96dbec24ac64e7dd5fef6e2c26214c8fe5be3486d5c92d21d5dcb4f6c4e365b9, adba167a9df482aa991faaa0e0cde1182fb9acfbb0dc8d19148ce634608bab87, c1a0d380bf55070496b9420b970dfc5c2c4ad0a598083b9077493e8b8035f1e9, e315907415eb8cfcf3b6a4cd6602b392a3fe8ee0f79a2d51a81a928dbce950f8, fe07ca449e99827265ca95f9f56ec6543a4c5b712ed50038a9a153199e95a0b7, 5460b51da26c060727d128f3b3d6415d1a4c25af6a29fef4cc6b867ad3659078
MD5	089801d87998fa193377b9bfe98e87ff, 0c1554888ce9ed0da1583dbdf7b31651, 12b5e30c2276664e87623791085a3221, 427258462c745481c1ae47327182acd3, 5e4c62329612559225 6630deabdbf1d2, 724c8059c150b0f3d1e0f80370bcfe19, 87312a7173889a8a5258c68cac4817bd, a43e3cf908244f85b237fdbacd8d82d5, b9f5e9db9eec8d1301026c443363cf6b, d31ec83a5a79451a46e980ebffb6e0e8
SHA1	43bc39e341b3be62bd7841e8eba92aa91b4460e4, 248cd3b57835aeb8826cce3437582fb38da9f9fa, 3a2c6cc8c18e2de6a2256876358e7ff86651f043, dbf5066fd3d38c4478f746fb5c6de0b441e1b149, 3ad9be0c52510cbc5d1e184e0066d14c1f394d4d, 4ad043c8f37a916761b4c815bed23f036dfb7f77, 5592434c40a30ed2dfdba0a86832b5f2eaaa437c, 988fc0d23e6e30c2c46ccec9bbff50b7453b8ba9, a7c6f264b00d13808ceb76b3277ee5461ae1354e, d12b614e9417c4916d5c5bb6ee42c487c937c058, D7a8d8303361ffd124cb64023095da08a262cab4,

TYPE	VALUE
SHA1	e1e427c9b46064e2b483f90b13490e6ef522cc06, ef8036eb4097789577eff62f6c9580fa130e7d56, f99779a5c891553ac4d4cabf928b2121ca3d1a89
URLs	http://172[.]233[.]228[.]93/lowdp, http://172[.]233[.]228[.]93/policy, http://172[.]233[.]228[.]93/vpn[.]log, http://172[.]233[.]228[.]93/vpn_prot[.]gz, hxxp://172[.]233[.]228[.]93/policy, hxxp://172[.]233[.]228[.]93/patch
IPv4	137[.]118[.]185[.]101, 144[.]172[.]79[.]92, 172[.]233[.]228[.]93, 198[.]58[.]109[.]149, 23[.]242[.]208[.]175, 66[.]235[.]168[.]222, 71[.]9[.]135[.]100, 89[.]187[.]187[.]69

Patch Details

Upgrade PAN-OS software to:

PAN-OS 11.1: Hotfix 11.1.2-h3
PAN-OS 11.0: Hotfix 11.0.4-h1
PAN-OS 10.2: Hotfix 10.2.9-h1

Link:
https://security.paloaltonetworks.com/CVE-2024-3400

References

https://unit42.paloaltonetworks.com/cve-2024-3400/

https://www.cisa.gov/news-events/alerts/2024/04/12/palo-alto-networks-releases-guidance-vulnerability-pan-os-cve-2024-3400

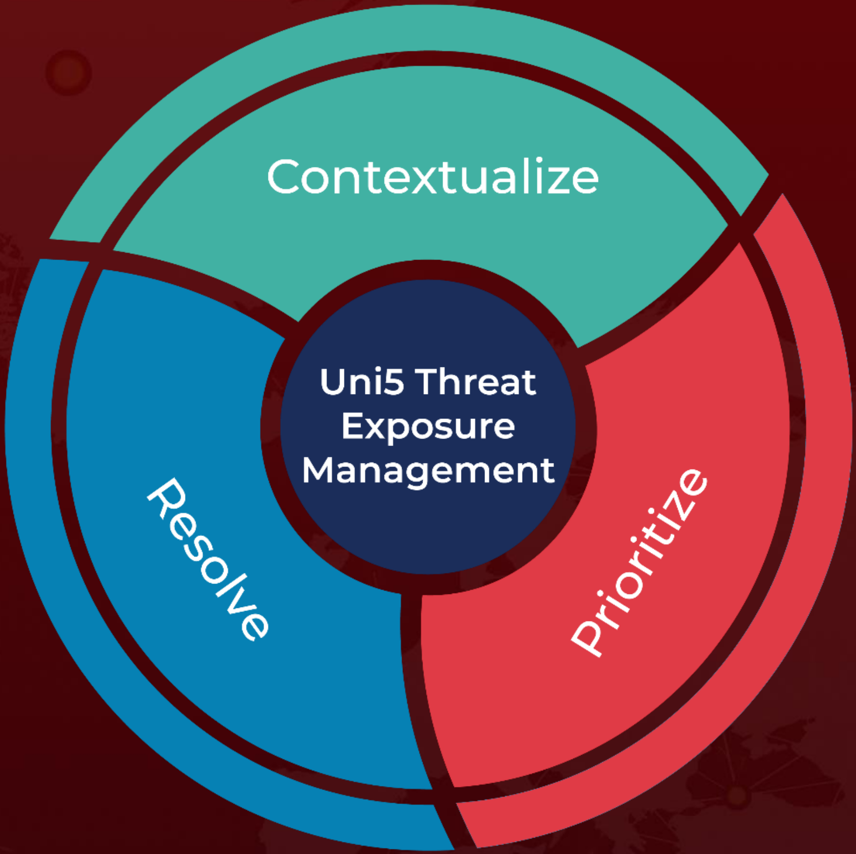
https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/

https://github.com/0x0d3ad/CVE-2024-3400

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 15, 2024 • 6:30 AM

More at www.hivepro.com