2024-04-18

HUNTER

EMERGING THREATS

CVE-2024-3400 - PALO ALTO OS COMMAND INJECTION VULNERABILITY

CVE-2024-3400 is a unauthenticated remote code execution vulnerability identified in devices utilizing GlobalProtect, and was identified by Volexity Threat Researchers on April of 2024. Reported to impact PAN-OS firewalls running versions 10.2, 11.0 and 11.1, this security flaw has been observed to be actively exploited (since March 26th) and considered critical in nature - Palo Alto Networks and Unit 42 labeling its exploitation as Operation MidnightEclipse. When exploited, it allows malicious actors to execute arbitrary code as a privileged user on the victim's firewall - with initial post exploitation being observed to include the utilization of a reverse shell, downloading of tools and subsequent lateral movement within the targeted environment.

THREAT SUMMARY

CVE-2024-3400 is a unauthenticated remote code execution vulnerability identified in devices utilizing GlobalProtect, and was identified by Volexity Threat Researchers on April of 2024. Reported to impact PAN-OS firewalls running versions 10.2, 11.0 and 11.1, this security flaw has been observed to be actively exploited (since March 26th) and considered critical in nature - Palo Alto Networks and Unit 42 labeling its exploitation as Operation MidnightEclipse. When exploited, it allows malicious actors to execute arbitrary code as a privileged user on the victim's firewall - with initial post exploitation being observed to include the utilization of a reverse shell, downloading of tools and subsequent lateral movement within the targeted environment.

Consequently, Palo Alto networks began releasing hotfixes to help secure firewalls exposed to the vulnerability. They are urging customers who are utilizing these exploitable versions of PAN-OS, to upgrade as soon as possible to fixed versions they have released ([More Information from Palo Alto Found Here] (https://unit42.paloaltonetworks.com/cve-2024-3400)).

SYNOPSIS

In April 2024, Volexity discovered zero-day exploitation(s) of a vulnerability found within Palo Alto PAN-OS firewalls, more specifically those that are running versions 10.2, 11.0 and 11.1. This vulnerability was given the designation of CVE-2024-3400, and given the CVSS score of 10.0 (Critical). Discovered to be an OS command injection issue, exploitation of CVE-2024-3400 allows a malicious actor unauthorized root privileges on the firewall - allowing the execution of arbitrary code.

Volexity researchers observed the threat actor (named UTA0218) " remotely exploit the firewall device, create a reverse shell, and download further tools onto the device"(Volexity, 2024). Furthermore, after the malicious actor exploits the vulnerability, researchers saw the deployment of the python-based UPSTYLE backdoor that equipped the actor(s) with a means to execute commands on devices that were compromised. This was observed with the creation/manipulation of a path configuration file (system.pth) to execute code every time Python starts - monitoring access logs to pick out base64 commands. In an observed an instance of post-exploitation, the actor was able to pivot into internal resources via SMB and WinRM in order to exfiltrate windows data (such as the Active Directory Database for example) and proprietary data as well (such as stored credentials).

Given the severity of CVE-2024-3400 and the capabilities that are given to a malicious actor if successfully exploited (as well as the sheer number of potentially vulnerable Palo Alto firewalls susceptible to attack), it is important to assess, understand and adequately prepare for this vulnerability if your environment is potentially at risk.

HUNT PACKAGES

CURL/WGET DOWNLOAD AND EXECUTE – POTENTIAL PAYLOAD DOWNLOAD FOLLOWED BY EXECUTION
https://hunter.cyborgsecurity.io/research/hunt-package/b585a013-e56d-4c3f-ac29-f2a610ac0ce8

REMOTE INTERACTIVE CONNECTIONS FROM UNEXPECTED LOCATIONS
https://hunter.cyborgsecurity.io/research/hunt-package/e828d24d-e0c6-46aa-8ec3-ed528696276b

CURL/WGET ACTIVITY ASSOCIATED WITH TIME ZONE LOOKUPS
https://hunter.cyborgsecurity.io/research/hunt-package/41e0de2d-367e-484c-8763-4eded0d85226

USAGE OF CHMOD TO ENABLE EXECUTION – POTENTIAL PAYLOAD STAGING
https://hunter.cyborgsecurity.io/research/hunt-package/dfbdc565-a37c-472b-a4c7-6c0e5325b255

RELATED LINKS
Sign up for free HUNTER access
CVE-2024-3400 - Palo Alto OS Command Injection Vulnerability Emerging Threat Collection

MITRE CONTEXT

- Tactic Names:
  - Execution
  - Reconnaissance
  - Discovery
  - Lateral Movement
  - Command and Control
  - Defense Evasion
- Technique Names:
  - Linux and Mac File and Directory Permissions Modification
  - Command and Scripting Interpreter
  - Ingress Tool Transfer
  - System Location Discovery
  - Network Topology
  - Remote Services

- Threat Names:

REFERENCES

1. https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/
2. https://unit42.paloaltonetworks.com/cve-2024-3400/
3. https://www.bleepingcomputer.com/news/security/exploit-released-for-palo-alto-pan-os-bug-used-in-attacks-patch-now/
4. https://labs.watchtowr.com/palo-alto-putting-the-protecc-in-globalprotect-cve-2024-3400/