

CVE-2024-3400 Vulnerability

 enigmasoftware.com/cve20243400vulnerability-removal/



By **Mezo** in [Vulnerability](#)

Since March 26, 2024, threat actors have been taking advantage of a newly revealed zero-day vulnerability in Palo Alto Networks PAN-OS software. Dubbed Operation MidnightEclipse by researchers, this activity is attributed to a single unidentified threat actor.

The vulnerability, known as CVE-2024-3400 and rated with a CVSS score of 10.0, is a command injection flaw. It allows unauthenticated hackers to execute arbitrary code with root privileges on affected firewalls. Notably, this issue affects only PAN-OS 10.2, PAN-OS 11.0, and PAN-OS 11.1 configurations with GlobalProtect gateway and device telemetry enabled.

[Table of Contents](#)

Attackers Exploit the CVE-2024-3400 Vulnerability to Deliver a Backdoor Malware

Operation MidnightEclipse involves leveraging the vulnerability to establish a cron job that executes every minute, fetching commands from an external server ('172.233.228.93/policy' or '172.233.228.93/patch') and running them via the bash shell.

The attackers have reportedly manually controlled an access control list (ACL) for the Command-and-Control (C2) server, ensuring that only the communicating device can access it.

While the precise function of the command remains unclear, it is suspected to serve as a delivery mechanism for a Python-based backdoor dubbed UPSTYLE by researchers tracking the exploitation of CVE-2024-3400. This backdoor is hosted on a separate server ('144.172.79.92' and 'nhdata.s3-us-west-2.amazonaws.com').

The Python file is designed to create and execute another Python script ('system.pth'), which in turn decodes and launches the embedded backdoor component responsible for executing the threat actor's commands. The results of these operations are logged in a file named 'sslvpn_ngx_error.log,' while another file named 'bootstrap.min.css' records additional activity.

Attackers Seek to Harvest Sensitive Information from Infected Devices

A notable aspect of the attack chain is the utilization of legitimate files associated with the firewall for both extracting commands and logging results:

- /var/log/pan/sslvpn_ngx_error.log
- /var/appweb/sslvpn/docs/global-protect/portal/css/bootstrap.min.css

To write commands to the Web server error log, the threat actor crafts specific network requests targeting a nonexistent web page with a particular pattern. Subsequently, the backdoor scans the log file for lines matching a predefined regular expression ('img[([a-zA-Z0-9+/=]+)]') to decode and execute embedded commands.

Additionally, the script spawns a new thread to execute a function named 'restore.' This function restores the original content and access/modified times of the bootstrap.min.css file after a 15-second delay, effectively erasing traces of command outputs.

The primary objective seems to be minimizing evidence of command execution, requiring the exfiltration of results within 15 seconds before file overwrite.

Researchers have observed the threat actor remotely exploiting the firewall to establish a reverse shell, acquire additional tools, penetrate internal networks, and ultimately extract data. The exact scope of the campaign remains uncertain. The actor has been dubbed UTA0218, showcasing advanced capabilities and rapid execution indicative of a skilled threat actor with a predefined strategy to achieve their goals.

Initially, UTA0218 focused on acquiring domain backup DPAPI keys and targeting active directory credentials to obtain the NTDS.DIT file. They also sought to compromise user workstations to steal saved cookies, login data, and DPAPI keys.

Organizations are advised to monitor for signs of internal lateral movement.

CISA Warns about the CVE-2024-3400 Vulnerability

The developments around the CVE-2024-3400 Vulnerability prompted the U.S. Cybersecurity and Infrastructure Security Agency (CISA) to include the flaw in its Known Exploited Vulnerabilities (KEV) catalog, mandating federal agencies to apply patches for mitigating potential threats.

Targeting edge devices remains a favored attack vector for skilled threat actors who need the necessary time and resources to explore new vulnerabilities.

Given the resources required to develop and exploit such a vulnerability, the nature of targeted victims, and the demonstrated capabilities in installing the Python backdoor and infiltrating victim networks, it is highly probable that UTA0218 is a state-backed threat actor.

Your comment is awaiting moderation.

Please verify that you are not a robot.

Loading...