ON2IT AND AMS-IX PRESENT: THREAT TALKS

SPECIAL

Threat Talks Special
Unraveling CVE-2024-3400

A Comprehensive Analysis of the Vulnerability

On April 12th, Palo Alto Networks initially shared information about CVE-2024-3400, a significant vulnerability within their PAN-OS software. Just a few days later, further details emerged, indicating a broader scope of potentially affected devices than initially anticipated.

In this special edition of Threat Talks, we delve into a critical cybersecurity development of CVE-2024-3400. What is it exactly? It's a high-risk vulnerability found in the GlobalProtect feature, carrying the maximum severity score of 10. Join us as we unpack the details of this serious security flaw and its implications for users worldwide.

In this special episode we will discuss the following scenarios:

- Command execution
- 'Running-config'
- Backdoor

PAN-OS
CVE-2024-3400 Exploitation

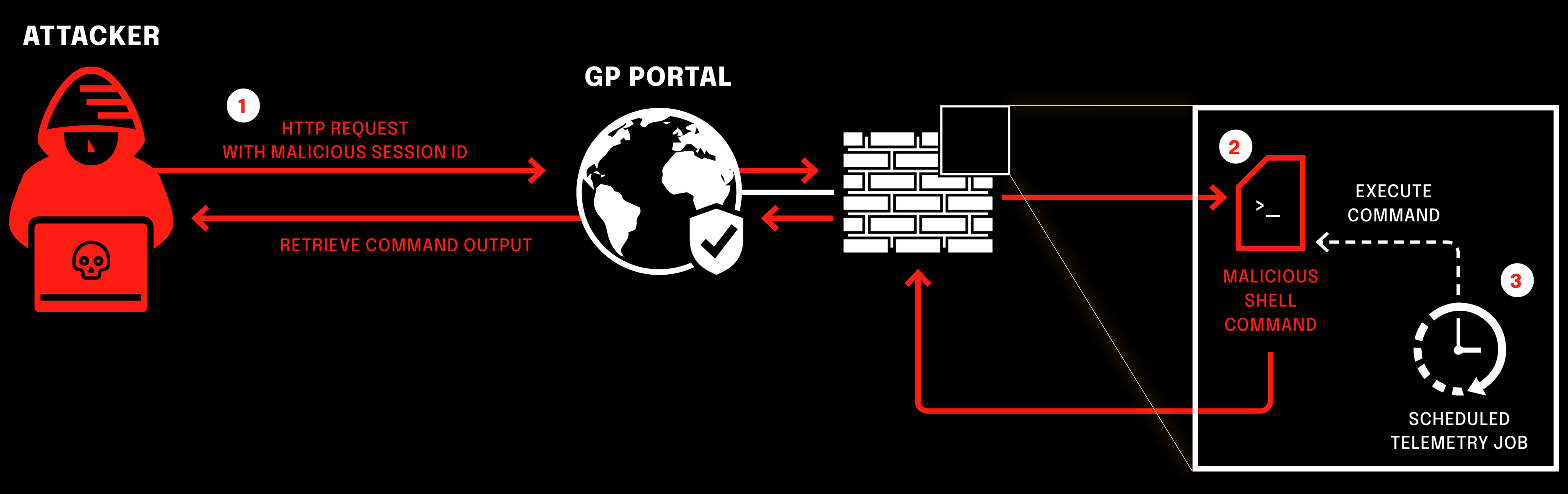
On April 12, 2024, a critical vulnerability, identified as CVE-2024-3400, was disclosed in PAN-OS. This flaw enables arbitrary file creation, leading to command injection in the GlobalProtect portal and gateway, allowing attackers to execute commands with root privileges. The vulnerability's severe impact is due to its network attack vector and low complexity, facilitating exploitation without user interaction. Forensic investigations on several companies have revealed signs of this vulnerability being exploited in the wild as early as March 26.

mSOC confidence score	Confirmed
Threat category	Vulnerability Disclosures - 0-days
Severity	Critical (CVSS score 10)

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1190 - Exploit Public-Facing Application	Exploit public face application to exfiltrate data and gain initial foothold	Code Obfuscation, Use of legitimate processes	Low	Enterprises, Government, Military

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1030 - Network Segmentation M1051 - Update Software M1016 - Vulnerability Scanning	Public Facing Access	Network traffic	Critical	Any

1A. Command Execution



HTTP Request

1. The attacker sends a HTTP request to GlobalProtect, with a manipulated SESSID cookie.

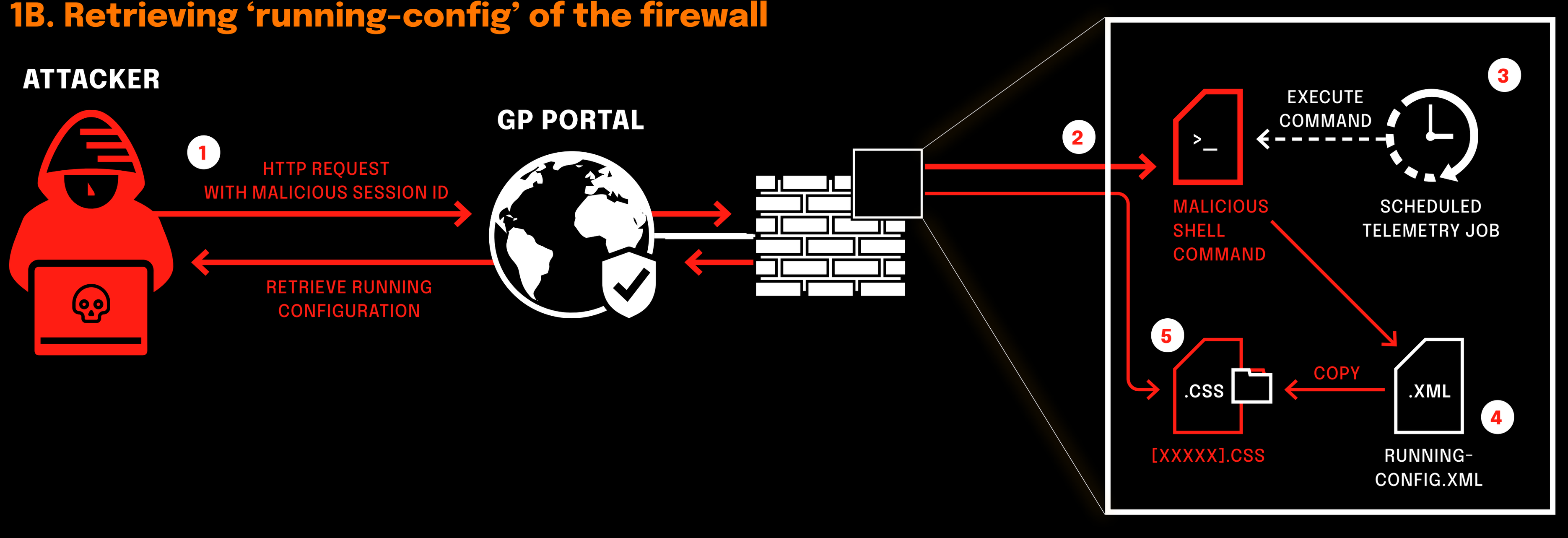
Malicious shell command

2. The web server normally saves data affiliated with unauthenticated sessions in /tmp/sslvpn, with a file named as the data contained in the cookie SESSID. By prepending a directory traversal to the SESSID data, the attacker is able to save the file with root privileges anywhere in the system, in this case in the telemetry subfolders

Scheduled Job

3. The telemetry scheduled job, trusting that the files were system-generated, uses the filenames as part of the command, resulting in the execution of the attacker-supplied code with elevated privileges. The output is then piped in a curl command connecting back to the attacker C2 server via DGA[1]

1B. Retrieving 'running-config' of the firewall



HTTP Request

1. As explained in the previous scenarios, the attacker sends a HTTP request to GlobalProtect, with a manipulated SESSID cookie.

Malicious shell command

2. By prepending a directory traversal to the SESSID data, the attacker saves a file with root privileges in the telemetry subfolders. This time the file name contains a base 64 encoded command.

Scheduled Job

3. Once the telemetry scheduled job runs, the command contained in the file name gets decoded and executed.

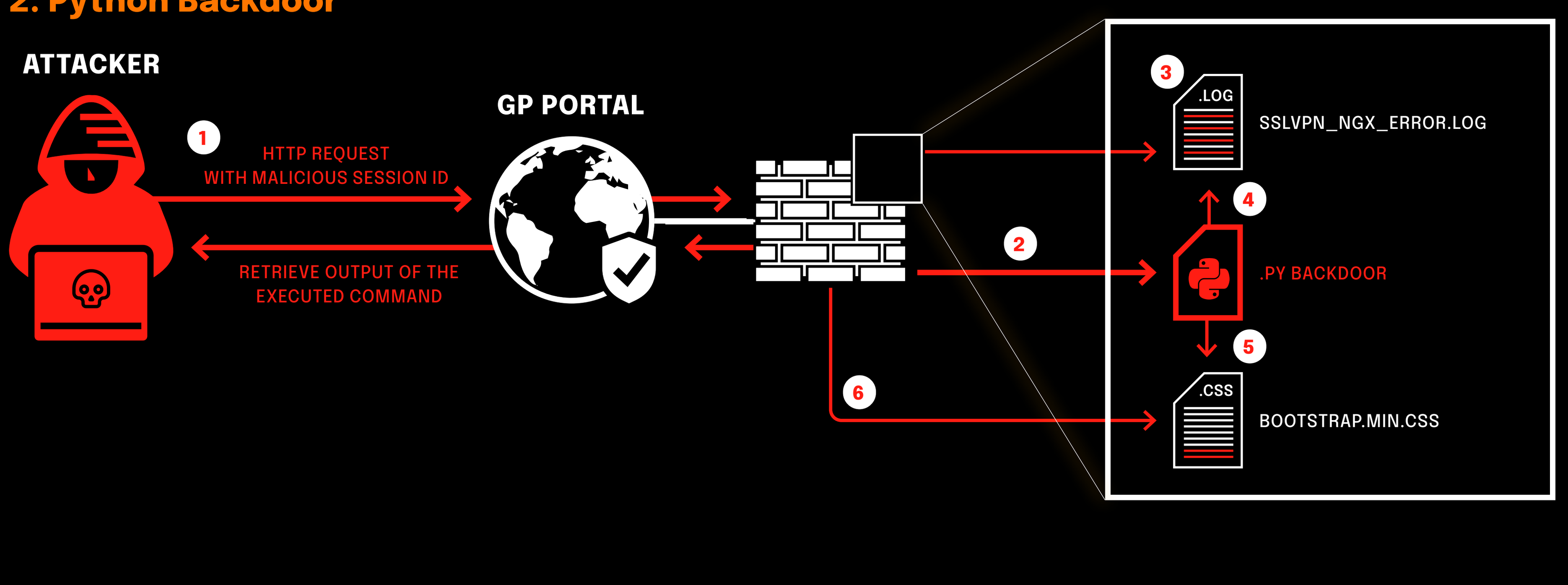
Copy of running-config

4. The command creates a copy of the firewall's running configuration and saves it as a new .css. The copy is placed in a folder accessible to the attacker (var/appweb/sslvpndocs/global-protect/).

Retrieve running configuration

5. At this point, the attacker retrieves the firewall's running configuration, which contains critical information such as admin accounts, hashed passwords, and secrets. If the firewall is configured with a default master key, cracking the encrypted data can be trivial for the attacker.

2. Python Backdoor



HTTP Request

1. As seen in attack A, the attacker sends an HTTP request to GlobalProtect with a malicious SESSID cookie, but this time the attacker creates a cron job in the cron.d folder.

Scheduled job execution

2. When the scheduled job executes, the firewall connects to a C2 server and installs a Python backdoor on the firewall. The main content of this backdoor is stored as a base64-encoded blob. By abusing a legitimate function in Python 3.5, the backdoor is configured to automatically start periodically.

Embedding commands

3. The attacker continuously sends HTTP requests to GlobalProtect, embedding commands that follow a specific pattern. These commands are also logged in /var/log/pan/sslvpn_ngx_error.log.

Log parsing

4. Periodically, the Python backdoor parses the logs in /var/log/pan/sslvpn_ngx_error.log, searching for a specific pattern, decoding them, and executing the commands. After command has been executed, the malicious entries are deleted from the sslvpn_ngx_error.log.

Append commands

5. The commands output is then appended to a legitimate .css file: /var/appweb/sslvpndocs/global-protect/portal/css/bootstrap.min.css, from where the attacker is able to retrieve the content.

Retrieve the output

6. At this point, the attacker retrieves the output from the bootstrap.min.css file. Fifteen seconds after the command is executed, bootstrap.min.css is restored to its original state.

[1] Domain Generation Algorithms (DGA) for C2 servers are used to avoid detection by creating numerous random domain names for command and control communications. This unpredictability complicates efforts to block malicious traffic. The domains often change daily based on algorithms that use seeds like the date.

Workaround / Solution

- Disabling telemetry stops the scheduled telemetry jobs from executing malicious commands, but it does not prevent arbitrary file writing.
- Palo Alto has released a content update featuring three different threat signatures to block exploitation of arbitrary file writing.
- For full mitigation, upgrading to a non-vulnerable version of PAN-OS is necessary.
- An extra solution could be to separate VPN features from the Firewall, essentially create a seperate zero trust protect surface for VPN access. This will result in less impact when such vulnerabilities are disclosed and more granular policies.

ON2IT - What the SOC did

Upon releasing the initial security advisory on April 12th, our mSOC™ swiftly communicated the details to all Strata customers via email. Simultaneously, the mSOC™ proactively applied all recommended mitigation measures, including threat content updates and disabling telemetry for all managed customers. Following this, Palo Alto Networks issued further bulletins clarifying that disabling telemetry alone was inadequate. They released additional updates to address the arbitrary write bug, which our mSOC™ promptly deployed to all managed customer systems upon the availability of new signatures. Palo Alto also provided a script to detect any exploit attempts on devices. The mSOC™ executed this script on all vulnerable devices and arranged a meeting with a Palo Alto Networks root engineer to secure forensic artifacts, and evaluate the extent of the attack, including any successful data extractions from the firewalls.

Taxonomy

ATT&CK Technique
Which technique of the MITRE ATT&CK framework does the threat correspond to.

ATT&CK Mitigation
Which mitigation of the MITRE ATT&CK framework can be applied.

Attack Strategy
Plan devised by the attacker to exploit specific system vulnerabilities.

Attack Vector
What is the primary method of attack.

Evasion
Tactics used by the attacker to avoid detection or bypass security.

Detection
Mechanism to identify malicious activities or system anomalies.

Complexity
How easy it is to exploit the vulnerability or carry out the attack.

Threat Level
How severe the threat is.

Target Type
The category of organization that may potentially be targeted.

Threat Actor Type
What type of threat actor may be involved.

CONTACT US

mSOC score explanation:
We assign scores to both our sources and the news items. Sources are scored on a numeric scale ranging from 0 (untrustworthy) to 5 (verified), while news items are scored with a letter, ranging from E (unreliable) to A (reliable). By considering the scores of both the source and the news item and the quality of the available information, we classify the overall reliability into three categories: Confirmed, Verified, and Credible. Interested in learning more about our reliability scoring system for sources and news items? Our Threat Intelligence team would be happy to walk you through our procedure, so please don't hesitate to reach out.

threat-talks.com

ON2IT ZERO TRUST INNOVATORS amsix