CrowdStrike Services

CrowdStrike Services

Critical Palo Alto Networks (PAN) GlobalProtect Vulnerability

Quick Reference Guide

Version 1.0.1

Dated: April 22, 2024

Table of Contents

Overview

On April 12, 2024, Palo Alto Networks (PAN) disclosed a command injection vulnerability present in the GlobalProtect component of certain versions of the PAN-OS operating system, which runs on PAN's Next-Generation Firewall (NGFW) appliances. Between April 14, 2024, and April 18, 2024, PAN remediated the vulnerability and released hotfixes for multiple PAN-OS versions. At the time of publication of this QRG, some older and less commonly deployed releases of PAN-OS still await a hotfix.

This vulnerability has been assigned the Common Vulnerabilities and Exposures (CVE) code `CVE-2024-3400` and a Common Vulnerability Scoring System (CVSS) severity level of 10/10 for its relative low complexity and high impact.[1] A CVSS score of 10/10 is the highest severity rating that can be given to a vulnerability. The score is based on a variety of factors that determine the vulnerability's impact.

Vulnerable Versions of PAN-OS

The most recent information about versions of PAN-OS vulnerable to `CVE-2024-3400` is available on PAN's Security Advisories page.[2] A list of vulnerable PAN-OS versions can be found on the Palo Alto website: https://security.paloaltonetworks.com/CVE-2024-3400 .

Where a hotfix is not available for an impacted PAN-OS version, CrowdStrike recommends either keeping the appliance offline until a fix is available or installing a more recent PAN-recommended PAN-OS version, which includes the hotfix. For example, firewalls running PAN-OS version 11.0.1 should either be kept offline or upgraded to version 11.0.2-h4 or higher.

Initial Access and Post-Exploitation Activity

On April 10, 2024, the cybersecurity vendor Volexity published information about successful exploitation of CVE-2024-3400 dating back to March 26, 2024. Exploitation of this CVE allows an attacker to remotely execute commands as the root user on a vulnerable appliance. Unauthorized third parties ("threat actors") have used this exploit to gain an initial foothold in a target environment and used this position to perform a variety of tasks, including configuring persistence and downloading additional tooling.[3]

CrowdStrike has observed exploitation of this vulnerability by multiple threat actors, as exploit code is currently publicly available, who have a diverse range of objectives, including ransomware deployment and exfiltration of data in support of extortion operations. CrowdStrike predicts, with high confidence, that opportunistic and sophisticated threat actors alike will continue to target this vulnerability for the foreseeable future.

CrowdStrike recommends patching this vulnerability as soon as possible. Due to the ease of exploitation, it is likely that *GlobalProtect*-enabled NGFWs, which are currently online and vulnerable, will present indicators of compromise (IOCs) recorded in logs. These indicators may be simple scanning or full-on attempts to breach the affected network. Patching vulnerable NGFWs may not remove persistence that was created before the NGFW was patched — further recommendations are in the section Remediation of Exploitation and Follow-On Activity.

[1] To access PAN's information on this CVE, see https://security.paloaltonetworks.com/CVE-2024-3400.

[2] To access PAN's Security Advisories page, see https://security.paloaltonetworks.com.

[3] For additional information from Volexity, see https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400.

UPSTYLE BACKDOOR

Volexity identified a Python backdoor that reads and executes commands written to the *GlobalProtect Nginx* error log file (`/var/log/pan/sslvpn_ngx_error.log`), which match a unique pattern. Command output is temporarily written to the path of a legitimate style file (`bootstrap.min.css`), which is restored back to its factory default contents after 15 seconds. This allows the threat actor to perform remote code execution and fetch command outputs. A custom backdoor, which Volexity refers to as *UPSTYLE,* is used as a first-stage backdoor in conjunction with proxy/tunnelling tools such as GO Simple Tunnel (GOST).

Collection and Analysis

The following guidance will allow administrators to assess their systems for exploitation activity. CrowdStrike first recommends conducting a triage of two key *GlobalProtect* log files that can be collected in a tech support file from PAN NGFWs. If evidence of exploitation is found, or other indicators of malicious activity originating from a firewall have been identified, CrowdStrike recommends undertaking a more thorough review of the affected firewall by analyzing a forensic image of that firewall.

If a PAN NGFW device is impacted by exploitation of the vulnerability `CVE-2024-3400`, updating the PAN-OS version or factory resetting the device will destroy some, or all, of the forensic evidence required to investigate the full scope of Threat Actor activity on the device. **If you are engaged with CrowdStrike Services for a forensic investigation, please reach out to your CrowdStrike Project Manager prior to updating or resetting a PAN NGFW.**

To prevent lateral movement from impacted systems, while preserving evidence, a PAN NGFW affected by exploitation of the vulnerability `CVE-2024-3400` can be isolated either at the hypervisor level (if virtualized) or by removing any attached networking cables (if a physical appliance).

OBTAINING EVIDENCE FOR ANALYSIS

General guidance is provided first, followed by tailored advice for virtual and physical NGFWs. The first and most important step is to generate and download a tech support file for each vulnerable PAN NGFW.

GENERATE AND DOWNLOAD A TECH SUPPORT FILE FOR EACH VULNERABLE PAN NGFW

The management Command Line Interface (CLI) on a NGFW can be used to create a tech support file, which includes copies of a variety of artifacts that provide insight into potential exploitation. If you engage CrowdStrike Incident Response (IR) for support with a `CVE-2024-3400`-related security incident, the IR team will request these files for each vulnerable NGFW to rapidly triage possible attack activity.

PAN provides instructions to create tech support files on its website.[4] Follow the instructions and provide the output to your CrowdStrike project manager upon request so the data can be triaged. There is no need to provide the support files to PAN unless PAN specifically requests them as part of a separate support case.

Note that while tech support files can provide some information regarding exploitation attempts, they do not provide sufficient evidence for determining the full scope of activity if `CVE-2024-3400` exploitation is successful.

[4] For more information on creating PAN NGFW tech support files, see https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRlCAK.

If a threat actor has successfully compromised one or more NGFWs in your network, it is recommended to conduct further forensic analysis.

FULL DISK ANALYSIS: VIRTUAL FIREWALL APPLIANCES

A disk image, or a forensic copy, of virtual firewall storage can be exported from your virtualization infrastructure. CrowdStrike can typically work with virtual disk files. This can include Virtual Machine Disk (VMDK) and *Hyper-V* Virtual Hard Disk (VHDX) file types. Instructions are vendor-specific but can typically be found by searching for the name of your platform followed by "export disk image".

FULL DISK ANALYSIS: PHYSICAL FIREWALL APPLIANCES

CrowdStrike is aware of recommendations to remove hard drives from firewall appliances and create forensic images of them. If this is required during an IR engagement with CrowdStrike, this will be discussed and requested as needed. PAN may be able to support providing an image of the firewall, which can be provided to CrowdStrike for analysis.

LOG TRIAGE

With the caveat that exploitation of `CVE-2024-3400` provides a threat actor with `root` privileges on an impacted system, and access can potentially be used to remove indicators of exploitation, some triage guidance can be found below.

REVIEWING THE GLOBALPROTECT SERVICE LOG

One of PAN's threat brief blogs disclosing this vulnerability described an error message that is observable in the *GlobalProtect* service log (`gpsvc.log` and `gpsvc.log.old`). An example is shown in Figure .

```
{
    "level":"error",
    "task":"1234567-1",
    "time":"2024-04-01T00:00:00.000000000Z",
    "message":"failed to unmarshal session(EXPLOIT_ATTEMPT_HERE) map , EOF"
}
```

Figure 1: `gpsvc.log` Entry Showing Exploitation

The string within the parenthesis after `failed to unmarshal session` is an exploit command logged during attempts to inject commands via a malformed session identifier value, which triggers the vulnerability.

Due to the requirements for the exploit commands to work, the special variable `${IFS}` is used in place of a space. In a similar manner `${PATH:0:1}` has also been observed in some exploit attempts in place of a forward slash.

Exploit attempts observed include:

- Moving the `running-config.xml` file to the folder `/var/appweb/sslvpndocs/global-protect/portal/css/` with a `.css` extension
- Running a reverse shell
- Downloading additional tooling
- Setting up additional persistence via `cron` jobs

A disk image, or further forensic collection, is required to scope further activity regarding the impact of successful exploitation attempts.

REVIEWING THE GLOBALPROTECT WEB ACCESS LOG

The *GlobalProtect* application runs behind an *Nginx* web proxy. All incoming HTTP requests directed to the *GlobalProtect* component are recorded in the log file `sslvpn-access.log`. An example log entry showing exploitation is provided in Figure 2.

```
XXX.XXX.XXX.XXX  [2024-04-01 00:00:00.000000000 +0000 UTC] GET /global-
protect/login.esp HTTP/1.1 0 200 74, taskid 1234567
```

Figure 2: GlobalProtect NGINX Access Log sslvpn-access.log

Using the timestamp in square brackets, it is possible to match up and correlate error entries in the *GlobalProtect* service log file (`gpsvc.log`) with the threat actor's IP address. An exploitation attempt will initially generate an event log entry in the *NGINX* log `sslvpn-access.log` (example shown in Figure 2: GlobalProtect NGINX Access Log sslvpn-access.log). Afterward, an `unmarshal` error will be created in the *GlobalProtect* service log `gpsvc.log` (example shown in Figure) once the web request has been forwarded from *Nginx* to the *GlobalProtect* application.

As the vulnerability is present in the handling of the session identifier (`SESSID`) cookie, exploitation attempts will not be apparent from the log file `sslvpn-access.log` alone, as header data is not included. Both log files are required to understand threat actor activity.

Remediation

REMEDIATION OF THE VULNERABILITY

PAN began releasing hotfixes for affected versions of PAN-OS on April 14, 2024. A full chart can be found on PAN's customer support page for vulnerability `CVE-2024-3400`.[5]

REMEDIATION OF EXPLOITATION AND FOLLOW-ON ACTIVITY

If `CVE-2024-3400` was exploited prior to the vulnerability being patched, it is possible that a threat actor may have downloaded or configured additional tooling or persistence methods on a vulnerable firewall.

Updating the PAN-OS version may not be sufficient to remove persistence or threat actor tooling already present on impacted NGFWs. If exploitation of the vulnerability has occurred, CrowdStrike recommends following these steps to remediate affected appliances.

Where possible, CrowdStrike recommends taking the following steps on each impacted firewall:

1. Isolate impacted systems.
2. Export configuration data from the system. Verify expected data is present within the export.

[5] For more information, see https://security.paloaltonetworks.com/CVE-2024-3400 .

3. Factory reset physical device or create a new VM.
4. Import exported configuration data to the reset physical appliance or newly created PAN-OS VM.
5. If using a VM, freeze or pause the original appliance in the hypervisor to disconnect it from the network, while preserving its state for analysis.
6. Update each new system to the latest version provided by PAN.
7. Verify that all configurations expected on the device are correct and unmodified, paying attention to firewall rules and the *GlobalProtect* settings.
8. After verification, bring the clean and patched devices back into production.

Please note that, at this time, CrowdStrike cannot confirm whether a factory reset of a PAN firewall appliance completely removes all post-exploitation artifacts and/or threat actor-related persistence.

REMEDIATING FIREWALL-RELATED CREDENTIALS

Exploitation of `CVE-2024-3400` can expose credentials configured on the device to threat actors. CrowdStrike recommends auditing usage of any accounts, keys and identities that are configured on impacted NGFWs and changing these credentials.

Example credentials include:

- Active Directory (AD) accounts used for binding NGFWs to AD for user authentication via LDAP.
- RADIUS pre-shared keys (PSKs) used for authenticating users against authentication servers.
- Local user accounts (including “break glass” and administrator accounts) within the firewall’s local directory.

CrowdStrike Services

If you require additional assistance, please reach out to CrowdStrike's support team at **support@crowdstrike.com** or contact us via phone:

Americas/Canada	+1 888 512 8906
UK/Ireland	+44(0) 118 453 0400
Australia/New Zealand/APAC	(+61) 1300 245 584
Middle East/Turkey/Africa	+9714 429 5829

If further help is required and you would like to engage CrowdStrike's Incident Response team, please contact Professional Services by completing the form on **https://www.crowdstrike.com/experienced-a-breach**, or contact us via phone:

Americas/Canada	+1 855 276 9347
UK/Ireland	+44(0) 800 0487187
France	+33 801840073
Germany	+49 (0800) 3252669
Australia	(+61) 1800 290 853
Japan	+81 800 170 5401
India	+91 1800 040 3447
Saudi Arabia	+966 8008803012
UAE	+971 8000320534
Qatar	+974 800101302

Customers with an active CrowdStrike Services retainer should notify the Services team in accordance with the process outlined in your retainer agreement.

CrowdStrike — the world's leader in endpoint protection. We stop breaches.