CERT-EU

Security Advisory 2024-037

Critical Vulnerability in PAN-OS software

April 29, 2024 — v1.3

TLP:CLEAR

History:

- *12/04/2024 — v1.0 – Initial publication*
- *16/04/2024 — v1.1 – Add patch information*
- *17/04/2024 — v1.2 – Add information about vulnerable configurations, and detection opportunities*
- *29/04/2024 — v1.3 – Update recommendations and detection opportunities*

Summary

On April 12, 2024, Palo Alto Networks released a security advisory for a critical vulnerability affecting a feature of PAN-OS software. This vulnerability allows an unauthenticated remote attacker to execute arbitrary code as root on the affected device [1].

This vulnerability is **being exploited in the wild**, and proof-of-concepts have been publicly disclosed by third parties [4]. The vendor is gradually releasing patches for the vulnerable versions since April 14, 2024. However, the patches are not available for all the affected versions yet. In this case, it is highly recommended to apply the mitigation measures, as well as implementing the verification steps suggested by the vendor.

Technical Details

The vulnerability tracked as **CVE-2024-3400** and with a **CVSS score of 10.0** is a command injection vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software. If exploited, it may allow an unauthenticated remote attacker to execute arbitrary code with root privileges on the firewall.

Affected Products

The following product versions are affected:

- PAN-OS 11.1 before version 11.1.2-h3
- PAN-OS 11.0 before version 11.0.4-h1
- PAN-OS 10.2 before version 10.2.9-h1
- PAN-OS 10.2 before version 10.2.8-h3
- PAN-OS 10.2 before version 10.2.7-h8

Contrary to the initial statements, this issue is applicable only to affected versions of the product configured with GlobalProtect gateway or GlobalProtect portal (or both). Device telemetry does not need to be enabled for PAN-OS firewalls to be exposed to attacks related to this vulnerability. One can verify whether the GlobalProtect gateway or GlobalProtect portal is configured by checking for entries in the firewall web interface (Network > GlobalProtect > Gateways or Network > GlobalProtect > Portals) [1].

Recommendations

[Updated] CERT-EU strongly recommends taking remediation actions depending on the exploitation level found on affected devices [5]:

- **Level 0 - probing**: Unsuccessful exploitation attempt.
  - Update to the latest PAN-OS hotfix;
  - Create a master key [6], and elect AES-256-GCM [7].
- **Level 1 - test**: Vulnerability being tested on the device, a 0-byte file has been created and is resident on the firewall, no indication of any known unauthorised command execution.
  - Update to the latest PAN-OS hotfix.
  - Create a master key [6], and elect AES-256-GCM [7].
- **Level 2 - potential exfiltration**: 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`. The suggested remediation will eliminate the possibility of capturing forensic artefacts.
  - Engage incident response and isolate the device to be able to determine what was done on the device.
  - Once it is done, update to the latest PAN-OS hotfix and perform a Private Data Reset [8].
- **Level 3 - interactive access**: Interactive command execution: May include shell-based back doors, introduction of code, pulling files, running commands. The suggested remediation will eliminate the possibility of capturing Forensic Artifacts.
  - Engage incident response and isolate the device to be able to determine what was done on the device, and in the network (in case of lateral movement).
  - Once it is done, update to the latest PAN-OS hotfix and perform a Factory Reset [8].

[Updated] To identify the exploitation level of a device, it is advised following the verification steps suggested by the vendor described below [1]. Some mitigation steps are also available, and are described below.

Threat Prevention Based Mitigation

Customers with a Threat Prevention subscription can block attacks for this vulnerability by enabling Threat ID 95187 (introduced in Applications and Threats content version 8833-8682).

In addition to enabling Threat ID 95187, customers must ensure vulnerability protection has been applied to their GlobalProtect interface to prevent exploitation of this issue on their device [2].

Detection Opportunities

The following command can be used from the PAN-OS CLI to help identify indicators of exploit activity on the device [1]:

```
grep pattern "failed to unmarshal session(.\+.\/" mp-log gpsvc.log*
```

Benign `failed to unmarshal session` error logs typically appear like the following entry:

```
"message":"failed to unmarshal session(01234567-89ab-cdef-1234-567890abcdef)"
```

If the value between `session(` and `)` does not look like a GUID (the format shown above), but instead contains a file system path, this indicates the need for further investigation and the log entry could be related to the successful or unsuccessful exploitation of CVE-2024-3400.

[New] Additional information provided by Volexity [9] and Unit42 [4] could be used to determine the exploitation level of an affected device.

References

[1] https://security.paloaltonetworks.com/CVE-2024-3400

[2] https://live.paloaltonetworks.com/t5/globalprotect-articles/applying-vulnerability-protection-to-globalprotect-interfaces/ta-p/340184

[3] https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/device-telemetry/device-telemetry-configure/device-telemetry-disable

[4] https://unit42.paloaltonetworks.com/cve-2024-3400/

[5] https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000CrO6CAK

[6] https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/configure-the-master-key

[7] https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/master-key-encryption/configure-the-master-key-encryption-level#ida38d799c-29bb-4b3e-a7fd-f968b8affa64:~:text=DOWNLOAD%20PDF-,Configure%20Master%20Key%20Encryption%20Level,-Previous

[8] https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000008XrDCAU

[9] https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/