Emergency Update Required - PAN-OS Root and Default Certificate Expiration

Dear Palo Alto Networks Customers,

This update impacts you if you have a Palo Alto Networks Firewall or Panorama used for any of the following services:

1. **Scenario 1**
    - Data redistribution (User-ID, IP-tag, User-tag, GlobalProtect HIP, and/or quarantine list)
    - URL PAN-DB private cloud (M-Series)
    - WildFire private cloud appliance (WF500/B)
2. **Scenario 2**
    - WildFire/Advanced WildFire Public Cloud
    - URL/Advanced URL Filtering
    - DNS Security
    - ThreatVault
    - AutoFocus

What's Changing:

On December 31, 2023, the root certificate and default certificate for Palo Alto Networks firewalls and appliances running PAN-OS software will expire. If you do not renew your certificates before they expire, your firewalls and Panorama appliances will no longer establish new connections to Palo Alto Networks cloud services, which will impact network traffic and potentially cause a network outage when existing connections terminate and attempt to reconnect due to network changes, configuration changes, or unforeseen events.

The root certificate will expire December 31 14:47:47 2023 GMT
The device certificate will expire December 31 20:14:14 2023 GMT

Target Upgrade Versions

The table below contains the target upgrade versions for both scenario 1a and scenario 2b.

Current PAN-OS Version	Upgrade Target Version
8.1	8.1.21-h2 8.1.25-h1 or greater
9.0	9.0.16-h5 or greater
9.1	9.1.11-h4 9.1.12-h6 9.1.13-h4 9.1.14-h7 9.1.16-h3 9.1.17 or greater
10.0	10.0.8-h10 10.0.11-h3 10.0.12-h3 or greater
10.1	10.1.3-h2 10.1.5-h3 10.1.6-h7 10.1.8-h6 10.1.9-h3 10.1.10 or greater
10.2	10.2.3-h9 10.2.4 or greater
11.0	11.0.0-h1 11.0.1-h2 11.0.2 or greater
11.1	11.1.0 or greater

All hotfix releases have been published for Firewalls, Panorama, WF500/B, and URL Pan-DB private cloud (M-series) appliances. For WF500/B and URL Pan-DB private cloud (M-series) appliances specifically, please use the following hotfix releases: **8.1.25-h2, 9.0.16-h6, 9.1.16-h4, 10.0.12-h4, 10.1.11-h3, and 11.0.3-h1**

Action Required:

You will need to complete the appropriate actions as described in one or both of the scenarios below, depending on the services you are using. Evaluate whether these expiring certificates impact your firewalls, Panorama appliances, or connected services based on the considerations below and take the required action where applicable.

Scenario 1

If you are a customer with Data redistribution (User-ID, IP-tag, User-tag, GlobalProtect HIP, and/or quarantine list) you will need to take one of the following two actions: (1a) upgrade your affected firewalls, and Panorama (Management and Log Collector modes), OR (1b) deploy Custom Certificates to your affected firewalls, and Panorama (Management and Log Collector modes).

If you are a customer with URL PAN-DB private cloud (M-Series), or WildFire private cloud appliance (WF500/B), you will need to take the following action: (1a) upgrade your affected firewalls, WF-500s, M-Series, and Panorama (Management and Log Collector modes).

- 1a) Upgrade your impacted firewalls, WF-500, M-Series, and Panorama

    i. If you do not have Custom Certificates installed, you must upgrade all of your firewalls, WF-500s, M-Series, and Panoramas (Management and Log Collector modes) that participate in data redistribution (User-ID, IP-tag, User-tag, GlobalProtect HIP, and/or quarantine list), URL PAN-DB private cloud (M-Series), and/or WildFire private cloud (WF500/B) to one of the PAN-OS versions in the Target Upgrade Version table above.

    ii. Customers must upgrade their WF-500/B appliance to the releases mentioned below:
        i. **Released**: 8.1.25-h2, 9.0.16-h6, 9.1.16-h4, 10.0.12-h4, 10.1.11-h3, and 11.0.3-h1

    iii. Customers must upgrade their URL PAN-DB private cloud (M-Series) appliances to the releases mentioned below:
        i. **Released**: 8.1.25-h2, 9.0.16-h6, 9.1.16-h4, 10.0.12-h4, 10.1.11-h3, and 11.0.3-h1

- 1b) Deploy Custom Certificates to your affected firewalls and Panorama

    - **Data redistribution (User-ID, IP-tag, User-tag, GlobalProtect HIP, and/or quarantine list)**: If all firewalls and Panorama on your network are running PAN-OS version 10.0 or above, you can switch to Custom Certificates for data redistribution instead of default device and root certificates. For more details on configuring Custom Certificates for data redistribution, refer to the following article, steps 8 & 9.

      Important:
        - You must switch to custom certificates on the data redistribution agent and client for secure server and client communications.
        - If you use data redistribution between firewalls and Prisma Access, you must also apply a hotfix or upgrade your impacted firewalls. You do not need to make changes to Prisma Access–you need only upgrade your firewalls to a targeted upgrade version.

    - **WildFire private cloud (WF500/B)**: Custom Certificates are not an option.

    - **URL PAN-DB private cloud (M-Series)**: Custom Certificates are not an option.

Scenario 2

If you are a customer with WildFire public cloud, Advanced WildFire public cloud, URL Filtering, Advanced URL Filtering, DNS Security, Threat Vault, or AutoFocus, you must perform one of the following three actions before your certificates expire on December 31, 2023: (2a) install a specific content update on your impacted firewalls and Panorama appliances OR (2b)

upgrade your impacted firewalls and Panorama appliances OR (2c) enable device certificates on your impacted firewalls and Panorama appliances.

- **2a) Install a specific content update on your affected firewalls and Panorama appliances**.
  You must install the following content update version (8776-8390 or later) on your firewalls and Panorama.
  - If you have automatic content configured, this update will be automatic
  - If you manually update your content, please update your content to the content version above

- 2b) Upgrade your affected firewalls and Panorama
  Upgrade your firewall and Panorama to one of the PAN-OS versions in the Target Upgrade Versions mentioned above.

- 2c) Enable Device Certificate on your affected firewalls and Panorama
  - If you have firewalls and Panorama appliances running PAN-OS 8.1, PAN-OS 9.0, or PAN-OS 9.1, we do not recommend that you use this option.
  - If you have firewalls and Panorama appliances running PAN-OS 10.0.5, PAN-OS 10.1.10, PAN-OS 10.2.5, or PAN-OS 11.0.2 or any later versions or releases, follow the instructions to enable the Device Certificate.

FAQ:

PanOS 9.1 will have an end-of-life support date of December 12, 2023. Will you continue to support PanOS after the date?

For customers with Pan-OS 9.1, which has end-of-life (EoL) support date of December 13, 2023, we are extending support for all customers until March 31, 2024. This is now reflected in our end-of-life summary page.

Is my Prisma Access deployment affected by this emergency update?

If you use data redistribution between firewalls and Prisma Access, then you must apply a hotfix or upgrade your impacted firewalls. You do not need to make changes to Prisma Access; you need only upgrade your firewalls to a targeted upgrade version because this customer advisory does not impact the Prisma Access service.

What will the impact on my network be if I do not upgrade my firewalls and Panorama to one of the versions above by December 31, 2023?

For Scenario 1:

- If you do not upgrade your impacted firewalls and Panorama appliances by December 31, 2023, your firewalls and Panorama appliances will no longer be able to establish new connections to data redistribution (User-ID, IP-tag, User-tag, GlobalProtect HIP, or quarantine list),
- URL PAN-DB private cloud (M-Series) appliances or WildFire private cloud (WF-500 or WF-500-B) appliances: If your existing connections terminate (such as when you make network or configuration changes or experience any unforeseen network events), you will experience an outage of the impacted services when they fail to reconnect due to expired certificates.

For Scenario 2:
If you do not complete the recommended actions above before December 31, 2023, your WildFire public cloud, Advanced WildFire public cloud, URL Filtering, Advanced URL Filtering, DNS Security, Threat Vault, and AutoFocus services will no longer be able to establish new connections after that date.

How can I check my firewalls and Panorama to ensure they have the new root certificate that expires on January 1, 2032?

If your firewalls run any of the targeted PanOS versions listed above (or a later version) in the **Target Upgrade Versions,** then you have the new root certificate installed.

How do I determine if my firewalls and Panoramas are configured with custom certificates?

Custom certificates for data redistribution (User-ID, IP-tag, User-tag, GlobalProtect HIP, and/or quarantine list) are supported starting from PAN-OS 10.0 and above versions. You can verify whether you are using default/custom certificates for data redistribution using the below commands.

Redistribution Agent

```
admin@10.0-New-AFW> show redistribution service status

Redistribution info:
        Redistribution service:                    up
        listening port:                          5007
        SSL config:                  Custom certificates
        back pressure is:                         off
        number of clients:                          2
```

Redistribution Client

```
admin@10.0-New-CFW> show redistribution agent state all

Agent: 92-uid-Agent(vsys: vsys1) Host: 10.46.196.49(10.46.196.49):5007
        Status                                      : conn:idle
        Version                                     : 0x6
        SSL config:                                 : Custom certificates
        num of connection tried                     : 1
```

Custom certificates for WildFire private cloud (WF-500 or WF-500-B) are available beginning in PAN-OS 8.1 and all later versions.

Certificate verification from PAN-OS CLI:

```
dmin@sjc-bld-smk01-esx13-t2-pavm02> show wildfire status channel private
…

Secure Connection: Custom Trusted CA, Custom Client Certificate

…
```

For data redistribution (User-ID, IP-tag, User-tag, GlobalProtect HIP, and/or quarantine list), in which order should I upgrade?

- Until December 31, 2023, the redistribution agent and the redistribution client can be running different versions and still continue to connect and communicate successfully.
- You do not need to upgrade all of your firewalls and Panorama appliances simultaneously but you should start with your Panorama appliance upgrades and then upgrade your firewalls.
- On December 31, 2023, all of your firewalls and Panorama appliances need to be running one of the targeted versions for your network to continue to connect and communicate successfully and to share mappings & tags as expected.

Does this certificate expiry impact the communication between Firewalls and Windows User-ID/Terminal Server Agents?

No. Firewalls use different certificates to communicate with User-ID and Terminal Server agents so this customer advisory does not impact communication between firewalls and Windows User-ID and Terminal Server agents.

Why do I see a notification popup even when I have taken the necessary action to prevent this issue?

The message is broadcasted to all devices regardless of version or the actions taken and will keep showing until you click on the checkbox in the bottom left of the popup saying **Do not show again** (this checkbox tick is saved per user, not per system, so every admin with their own credentials will have to do select it for their own account).
If all the corrective actions have been taken appropriately, it is safe to ignore the notification.

Thank you for your understanding.