VITAL CYBER

MCNC®

Falcon Cloud SSL Certificate Rotation Dashboard

Crowdstrike has created a dashboard for all client environments to track assets affected by the March 2026 certificate rotation. Assets on an outdated sensor version - and assets provisioned after March 16th, 2026 with an outdated sensor - will lose Crowdstrike's protection and visibility, so this issue is important to understand and address in your environment. This guide will walk through the information provided in the dashboard and how to use that information to ensure your assets remain protected.

Initial Access

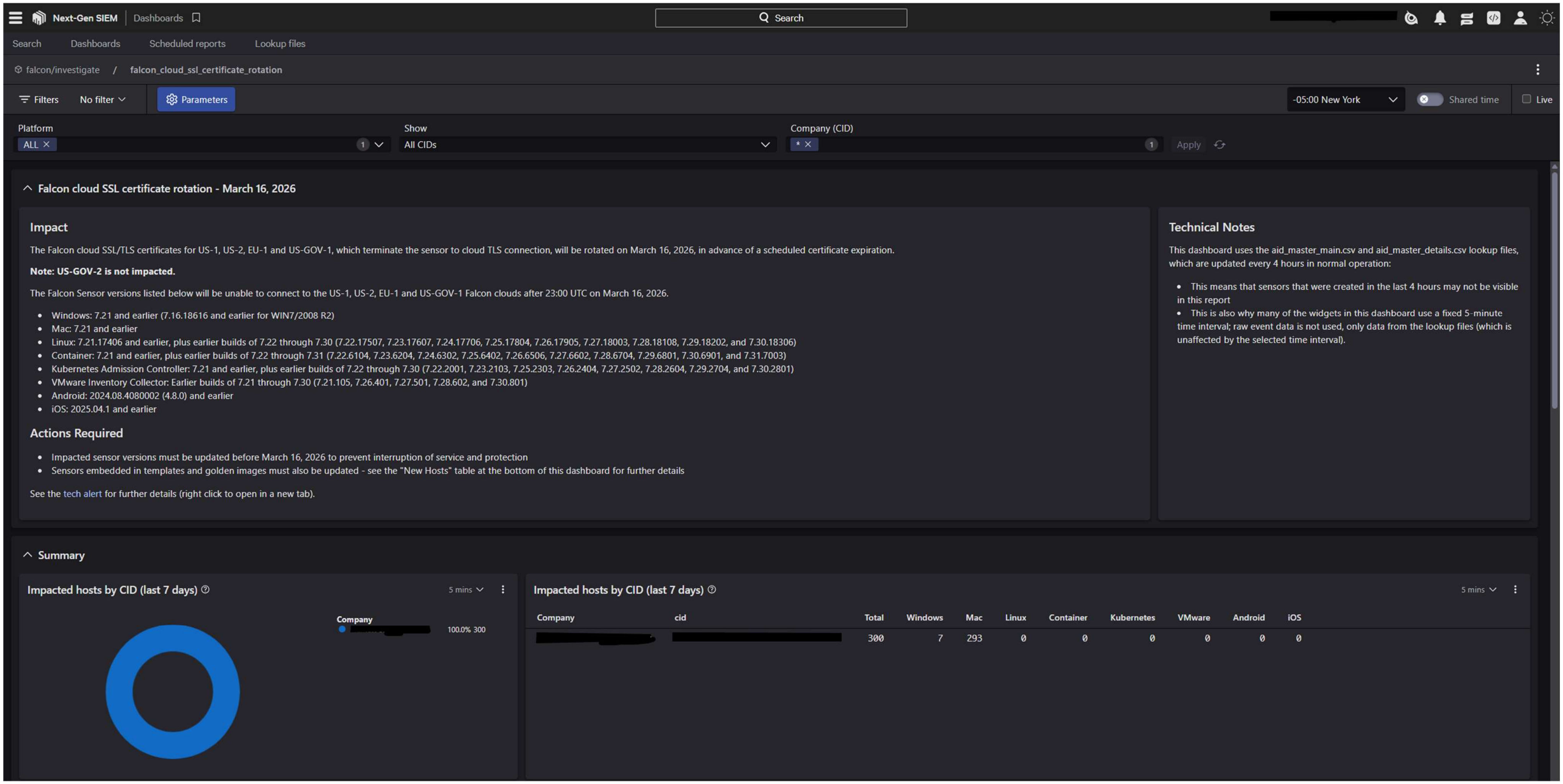
The Certificate Rotation Dashboard can be accessed via this generic, shareable link:

https://falcon.laggar.gcw.crowdstrike.com/investigate/search/custom-dashboards/falcon_cloud_ssl_certificate_rotation?packageScope=falcon%2Finvestigate&repoOrViewName=dashboards&sharedTime=false&start=1d

A Crowdstrike account is required to access the dashboard. If additional user accounts are needed, please reach out to secops@mcnc.org to create a ticket.

Overview

For demo purposes we are looking at a client dashboard with identifying data redacted. At the top are Impact and Technical Notes sections, which provide background, impacted sensor versions, required actions, and a link to a Support Portal article with additional information about the upcoming change. Below that are widgets showing hosts by CID (most clients will only have one) and operating system.



Platform: ALL ✕

Show: All CIDs

Company (CID): * ✕

Falcon cloud SSL certificate rotation - March 16, 2026

Impact

The Falcon cloud SSL/TLS certificates for US-1, US-2, EU-1 and US-GOV-1, which terminate the sensor to cloud TLS connection, will be rotated on March 16, 2026, in advance of a scheduled certificate expiration.

Note: US-GOV-2 is not impacted.

The Falcon Sensor versions listed below will be unable to connect to the US-1, US-2, EU-1 and US-GOV-1 Falcon clouds after 23:00 UTC on March 16, 2026.

- Windows: 7.21 and earlier (7.16.18616 and earlier for WIN7/2008 R2)
- Mac: 7.21 and earlier
- Linux: 7.21.17406 and earlier, plus earlier builds of 7.22 through 7.30 (7.22.17507, 7.23.17607, 7.24.17706, 7.25.17804, 7.26.17905, 7.27.18003, 7.28.18108, 7.29.18202, and 7.30.18306)
- Container: 7.21 and earlier, plus earlier builds of 7.22 through 7.31 (7.22.6104, 7.23.6204, 7.24.6302, 7.25.6402, 7.26.6506, 7.27.6602, 7.28.6704, 7.29.6801, 7.30.6901, and 7.31.7003)
- Kubernetes Admission Controller: 7.21 and earlier, plus earlier builds of 7.22 through 7.30 (7.22.2001, 7.23.2103, 7.25.2303, 7.26.2404, 7.27.2502, 7.28.2604, 7.29.2704, and 7.30.2801)
- VMware Inventory Collector: Earlier builds of 7.21 through 7.30 (7.21.105, 7.26.401, 7.27.501, 7.28.602, and 7.30.801)
- Android: 2024.08.4080002 (4.8.0) and earlier
- iOS: 2025.04.1 and earlier

Actions Required

- Impacted sensor versions must be updated before March 16, 2026 to prevent interruption of service and protection
- Sensors embedded in templates and golden images must also be updated - see the "New Hosts" table at the bottom of this dashboard for further details

See the tech alert for further details (right click to open in a new tab).

Technical Notes

This dashboard uses the aid_master_main.csv and aid_master_details.csv lookup files, which are updated every 4 hours in normal operation:

- This means that sensors that were created in the last 4 hours may not be visible in this report
- This is also why many of the widgets in this dashboard use a fixed 5-minute time interval; raw event data is not used, only data from the lookup files (which is unaffected by the selected time interval).

Summary

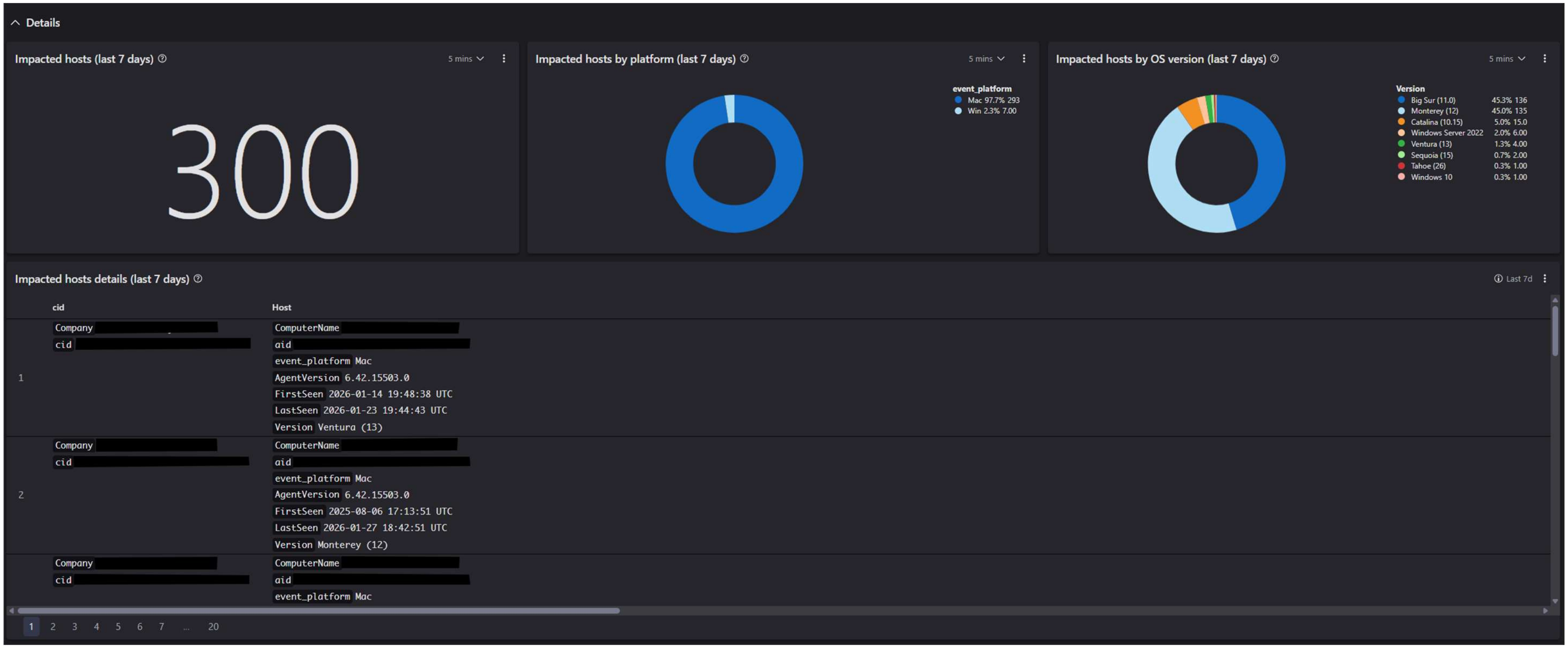
Impacted hosts by CID (last 7 days)

Impacted hosts by CID (last 7 days)

Company	cid	Total	Windows	Mac	Linux	Container	Kubernetes	VMware	Android	iOS
[redacted]	[redacted]	300	7	293	0	0	0	0	0	0

Impacted Hosts Details

Impacted Hosts Details shows any assets seen in your environment over the last 7 days using an unsupported sensor. These assets require direct remediation, as they have been unable to update to the correct version despite being on a Sensor Update policy created to maintain updates. The most common causes for update failure are assets running an OS no longer supported by Crowdstrike (supported Windows and MacOS versions can be referenced in the documentation) or assets that have been deployed using an installer that is no longer supported and unable to receive updates from Crowdstrike.



	cid	Host
1	Company [redacted] cid [redacted]	ComputerName [redacted] aid [redacted] event_platform Mac AgentVersion 6.42.15503.0 FirstSeen 2026-01-14 19:48:38 UTC LastSeen 2026-01-23 19:44:43 UTC Version Ventura (13)
2	Company [redacted] cid [redacted]	ComputerName [redacted] aid [redacted] event_platform Mac AgentVersion 6.42.15503.0 FirstSeen 2025-08-06 17:13:51 UTC LastSeen 2026-01-27 18:42:51 UTC Version Monterey (12)
	Company [redacted] cid [redacted]	ComputerName [redacted] aid [redacted] event_platform Mac

If you don't have any assets showing up in this dashboard, that's good! You should be aware that this dashboard only tracks assets that have been seen in the past 7 days, so it's recommended to check this dashboard regularly until March 16th so assets that are not regularly online can be identified and addressed.

For assets that do show up here, the resolution will depend on the root cause of the issue which may not be immediately apparent. Assets confirmed to be on an unsupported operating system should be updated to a supported OS if possible – this may allow the sensor to resume updating automatically, in which case no further action is needed. If an OS update does not resolve the issue or you've confirmed the OS is already supported, an uninstall and reinstall of the sensor using a current installer may be necessary. If neither of these actions solve the issue, please open a ticket by emailing secops@mcnc.org so we can investigate and work with Crowdstrike Support to resolve.

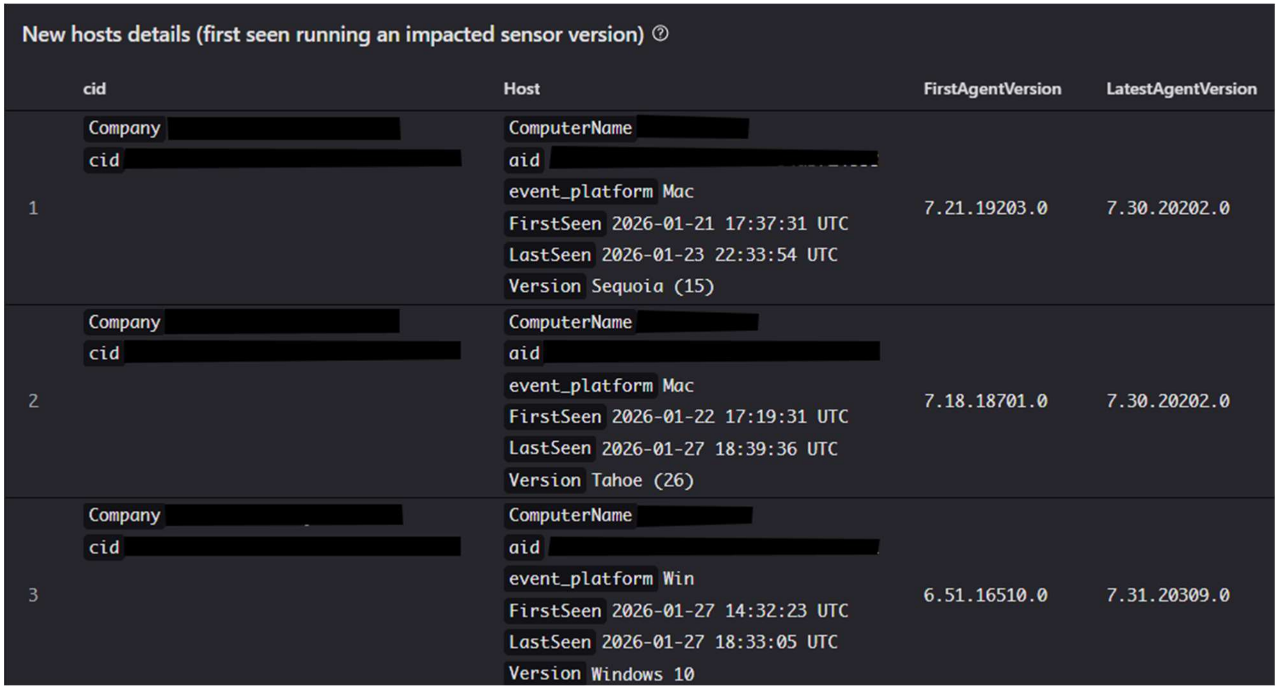
Quick Refresher: Uninstalling and reinstalling the sensor

1) For assets in standard policies, a maintenance token will be required*. These tokens can be found in Host Management by selecting the desired host, clicking the 'Actions' button on the right-hand side, and selecting 'Reveal Maintenance Token'.
2) **Windows**: The sensor can be uninstalled via Add/Remove Programs or via command line (docs). Paste the maintenance token when prompted (or include in command prompt).
   MacOS: The sensor can be uninstalled via Terminal. (docs) Paste maintenance token when prompted.
3) To reinstall, navigate to Sensor Downloads and download the latest release for your OS. Copy your customer ID string from the 'How to Install' instructions on the right. Run the installer and paste the customer ID when you are prompted.

**Note If you are uninstalling a large number of sensors, reach out to MCNC Support to move assets to a less restrictive uninstall policy. This will allow you to uninstall without requiring a unique uninstall token for each device*

New Hosts Details

‘New hosts details (first seen running an impacted sensor version)’ indicates newly seen hosts that were first seen running an unsupported sensor, though they have since been successfully updated via the Sensor Update policy. As a result, no immediate action is needed on the hosts in this list. However, initial observation on an unsupported version likely indicates that something in your deployment process needs to be updated. The specifics will depend on how you deploy Crowdstrike – there could be an outdated installer in a gold image or template, or you could be installing manually from an older version being stored on a network drive. If these installers are not updated in your deployment process before March 16th, hosts deployed using that method will no longer be able to automatically update, leading to a loss of protection and visibility for those assets.



New hosts details (first seen running an impacted sensor version)

	cid	Host	FirstAgentVersion	LatestAgentVersion
1	Company [redacted] cid [redacted]	ComputerName [redacted] aid [redacted] event_platform Mac FirstSeen 2026-01-21 17:37:31 UTC LastSeen 2026-01-23 22:33:54 UTC Version Sequoia (15)	7.21.19203.0	7.30.20202.0
2	Company [redacted] cid [redacted]	ComputerName [redacted] aid [redacted] event_platform Mac FirstSeen 2026-01-22 17:19:31 UTC LastSeen 2026-01-27 18:39:36 UTC Version Tahoe (26)	7.18.18701.0	7.30.20202.0
3	Company [redacted] cid [redacted]	ComputerName [redacted] aid [redacted] event_platform Win FirstSeen 2026-01-27 14:32:23 UTC LastSeen 2026-01-27 18:33:05 UTC Version Windows 10	6.51.16510.0	7.31.20309.0

Questions?

If you have any questions about the Certificate Rotation Dashboard, need assistance interpreting the data, or would like to discuss remediation in your environment, please reach out to MCNC Security Operations:

Email: secops@mcnc.org
Phone: 919-248-4141