

Dashboards to identify Windows hosts impacted by the content update defect

Published Date: Jul 20, 2024

Objective

- Updated dashboards are available to show the status of Windows hosts potentially impacted by the content update described in this [Tech Alert](#). Use these dashboards to get visibility to assist remediating Windows hosts.

Applies To

- Falcon sensor for Windows
- Microsoft Windows
- Falcon Insight

Procedure

Two dashboards are available that contain the same information presented differently. They can be found in the Falcon Console at:

- Next-Gen SIEM > Log management > Dashboards
 - Search for Hosts_possibly_impacted_by_windows_crashes
 - Note: The Dashboard cannot be used with the "Live" button
- A different dashboard view of the same information is available at the below links:
 - [\[US-1\]](#) [\[US-2\]](#) [\[EU-1\]](#) [\[US-GOV-1\]](#)

To use this dashboard:

1. In the **Company** field, select a CID in your environment
 - a. If you have multiple CIDs (Falcon Flight Control) and the dashboard does not return any data, enter an asterisk (*) in the CID field to get data from all CIDs in your environment.
2. Click **Apply** to reload the dashboard. The dashboard displays a list of hosts that are potentially impacted by the content issue.
3. Optionally, filter by additional details:
 - a. In the **ComputerName** field, leave the asterisk (*) unchanged to see all hosts, or enter a computer name filter to see specific hosts.
 - b. In the **Status** field, leave the asterisk (*) unchanged to see all statuses, or select a status filter to see specific hosts.
 - c. Click **Apply** to reload the dashboard.

The screenshot shows the Next-Gen SIEM dashboard with the title "hosts_possiblely_impacted_by_windows_crash...". The interface includes a search bar, filters, and a parameters section. The main content area is divided into two panels: "Impacted Sensors" (labeled 1) and "Impacted CIDs and Channels" (labeled 2).

Impacted Sensors (labeled 1): This table displays sensor statuses and associated channel files. The columns include cid, aid, ComputerName, Status, FirstSeen, LastSeen, CFVersion, MaxCFVersion, LastSeenDelta, and Details. The status field is color-coded: green for OK, red for CHECK, and grey for UNKNOWN.

cid	aid	ComputerName	Status	FirstSeen	LastSeen	CFVersion	MaxCFVersion	LastSeenDelta	Details
1			OK	2024-07-09 17:06:08	2024-07-21 03:18:34	34	34	14m51s	Endpoint has latest c
2			OK	2024-07-16 20:08:11	2024-07-19 13:32:04	34	34	1d14h	Endpoint has latest c
3			OK	2024-07-09 00:05:24	2024-07-21 03:16:54	34	34	16m31s	Endpoint has latest c
4			OK	2024-07-02 12:20:14	2024-07-21 03:27:56	34	34	5m30s	Endpoint has latest c
5			OK	2024-03-19 00:55:31	2024-07-21 03:10:33	34	34	22m52s	Endpoint has latest c
6			OK	2024-07-19 18:36:39	2024-07-19 20:34:16	34	34	1d6h	Endpoint has latest c
7			CHECK	2024-06-26 08:51:31	2024-07-19 11:54:02	33	34	1d15h	Endpoint has impacted
8			CHECK	2024-07-12 12:38:14	2024-07-19 11:56:21	33	34	1d15h	Endpoint has impacted
9			CHECK	2024-07-17 00:52:20	2024-07-19 12:27:30	33	34	1d15h	Endpoint has impacted
10			OK	2024-07-19 21:39:34	2024-07-19 21:51:48	34	34	1d5h	Endpoint has latest c
11			CHECK	2024-07-12 12:30:28	2024-07-19 19:33:11	33	34	1d8h	Endpoint has impacted
12			UNKNOWN	2024-07-08 00:10:05	2024-07-19 00:47:18	24	24	1d17h	Endpoint has latest c

Impacted CIDs and Channels (labeled 2): This table shows the impacted channel file for each CID. The columns include cid, ImpactedChannel, and name.

cid	ImpactedChannel	name
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		

Dashboard Widgets:

- **Impacted Sensors** (labeled 1): Shows sensor statuses, along with what channel file the sensor contains. CFVersion shows the sensor's current channel file.
- **Impacted CIDs and Channels** (labeled 2): Shows which channel file is associated with the content update defect. The impacted channel file varies for each CID.

When prioritizing remediations, refer to the **Status** field first:

- **CHECK:** remediation is likely required.
 - The host has received the problematic channel file during the impact window.
 - The host may be in a reboot loop, sitting at the recovery console, or has otherwise been unable to reconnect to our cloud to receive the reverted channel file.
- **VERIFY:** verify the host state.
 - The host may require remediation. It is possible that this host is stuck in a reboot loop and has been unable to connect to the CrowdStrike cloud to receive the reverted channel file as it is reporting that the channel file version zero is in use (unknown).
- **OK:** no action required.
 - The host has received the channel file with the remediation for this issue and should not be impacted.
- **UNKNOWN:** the state cannot be determined using available telemetry and does not fall into any of the above categories

NOTE: Hosts that are unexpectedly offline, as indicated by the LastSeen and LastSeenDelta columns in the dashboard, may still warrant further investigation. Hosts with a LastSeen date and timestamp between 04:00 UTC and 05:30 UTC on July 19th, 2024 should be given priority for investigation.

Additional Information

Additional details:

- This dashboard currently includes hosts running Falcon sensor for Windows version 7.10 and earlier. These hosts are not impacted by the content issue and do not need to be remediated. We plan to remove them in a future update to the dashboard.
- Hosts remain in this dashboard even if the sensor is uninstalled. The dashboard shows previously observed hosts that cease to communicate with the CrowdStrike cloud within the search timeframe.
- We are aware of some instances of false positives for sensors in the “Impacted Sensors” pane. We will continue to update this dashboard for improved accuracy.