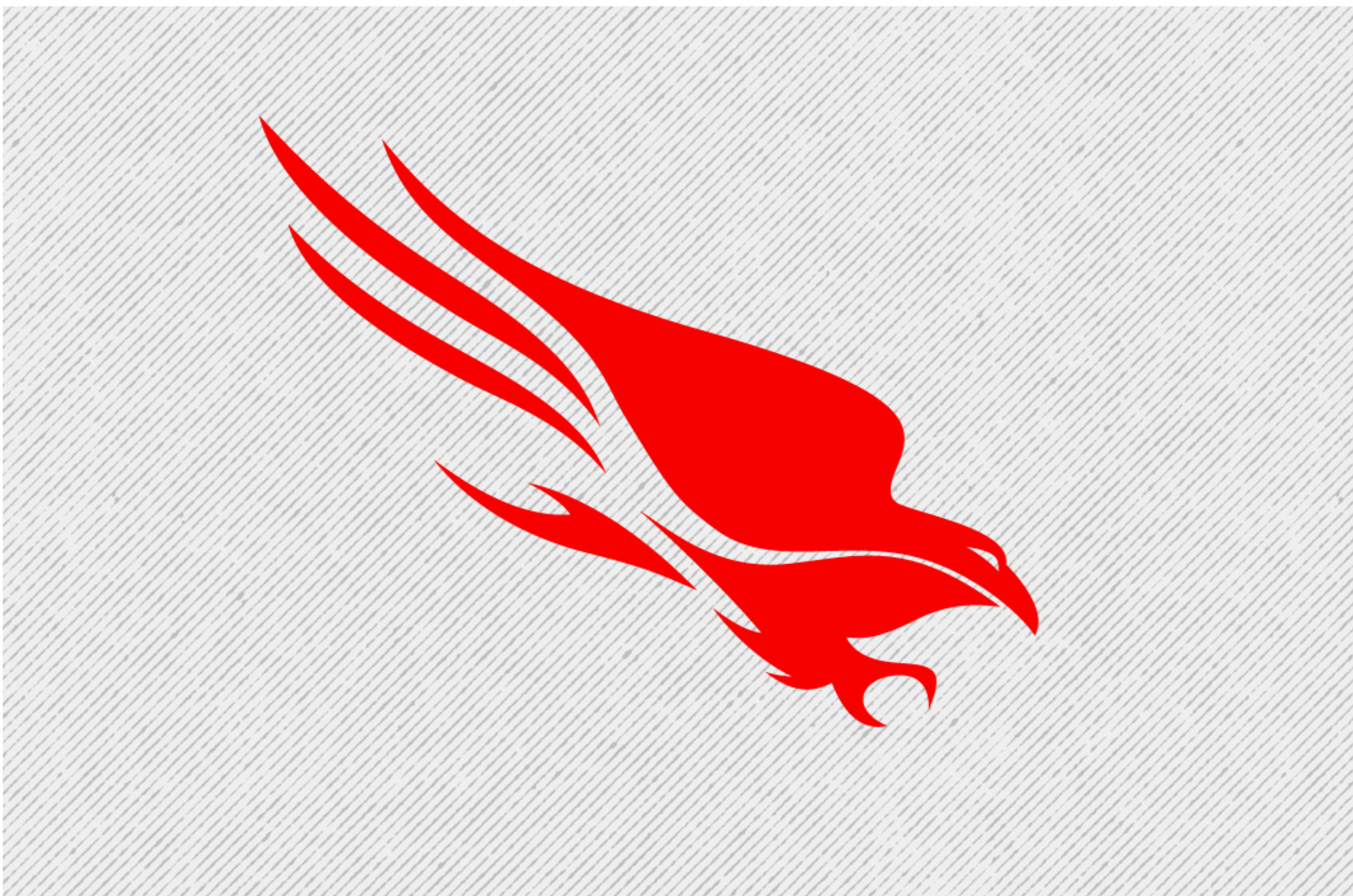


# Technical Details: Falcon Content Update for Windows Hosts

July 20, 2024 | [CrowdStrike](#) | [Executive Viewpoint](#)



## What Happened?

On July 19, 2024 at 04:09 UTC, as part of ongoing operations, CrowdStrike released a sensor configuration update to Windows systems. Sensor configuration updates are an ongoing part of the protection mechanisms of the Falcon platform. This configuration update triggered a logic error resulting in a system crash and blue screen (BSOD) on impacted systems.

The sensor configuration update that caused the system crash was remediated on Friday, July 19, 2024 05:27 UTC.

This issue is not the result of or related to a cyberattack.

## Impact

Customers running Falcon sensor for Windows version 7.11 and above, that were online between Friday, July 19, 2024 04:09 UTC and Friday, July 19, 2024 05:27 UTC, may be impacted.

Systems running Falcon sensor for Windows 7.11 and above that downloaded the updated configuration from 04:09 UTC to 05:27 UTC – were susceptible to a system crash.

## Configuration File Primer

The configuration files mentioned above are referred to as “[Channel Files](#)” and are part of the behavioral protection mechanisms used by the Falcon sensor. Updates to Channel Files are a normal part of the sensor’s operation and occur several times a day in response to novel tactics, techniques, and procedures discovered by CrowdStrike. This is not a new process; the architecture has been in place since Falcon’s inception.

## Technical Details

On Windows systems, Channel Files reside in the following directory:

`C:\Windows\System32\drivers\CrowdStrike\`

and have a file name that starts with “C-”. Each channel file is assigned a number as a unique identifier. The impacted Channel File in this event is 291 and will have a filename that starts with “C-00000291-” and ends with a `.sys` extension. Although Channel Files end with the `SYS` extension, [they are not kernel drivers](#).

Channel File 291 controls how Falcon evaluates named pipe<sup>1</sup> execution on Windows systems. Named pipes are used for normal, interprocess or intersystem communication in Windows.

The update that occurred at 04:09 UTC was designed to target newly observed, malicious named pipes being used by common C2 frameworks in cyberattacks. The configuration update triggered a logic error that resulted in an operating system crash.

## Channel File 291

CrowdStrike has corrected the logic error by updating the content in Channel File 291. No additional changes to Channel File 291 beyond the updated logic will be deployed. Falcon is still evaluating and protecting against the abuse of named pipes.

This is not related to null bytes contained within Channel File 291 or any other Channel File.

## Remediation

The most up-to-date remediation recommendations and information can be found on our [blog](#) or in the [Support Portal](#).

We understand that some customers may have specific support needs and we ask them to contact us directly.

Systems that are not currently impacted will continue to operate as expected, continue to provide protection, and have no risk of experiencing this event in the future.

Systems running Linux or macOS do not use Channel File 291 and were not impacted.

## Root Cause Analysis


We understand how this issue occurred and we are doing a thorough root cause analysis to determine how this logic flaw occurred. This effort will be ongoing. We are committed to identifying any foundational or workflow improvements that we can make to strengthen our process. We will update our findings in the root cause analysis as the investigation progresses.

<sup>1</sup> <https://learn.microsoft.com/en-us/windows/win32/ipc/named-pipes>


[✕ Tweet](#) [📄 Share](#)




### Related Content



#### To Our Customers and Partners













#### Statement on Falcon Content Update for Windows Hosts



#### CrowdStrike Unifies Threat Data and AI for Next-Gen Managed Detection and Response

### CATEGORIES

	Cloud and Application Security	95
	Counter Adversary Operations	178
	Endpoint Security & XDR	305
	Engineering & Tech	78
	Executive Viewpoint	158
	Exposure Management	80
	From The Front Lines	189
	Identity Protection	34
	Next-Gen SIEM & Log Management	84
	Public Sector	36

### CONNECT WITH US

[✕](#) [f](#) [@](#) [in](#) [v](#) [📧](#)

### FEATURED ARTICLES

- Tech Analysis: Channel File May Contain Null Bytes

July 24, 2024
- Lumma Stealer Packed with CypherIt Distributed Using Falcon Sensor Update Phishing Lure

July 24, 2024
- Preliminary Post Incident Review (PIR): Content Configuration Update Impacting the Falcon Sensor and the Windows Operating System (BSOD)


July 24, 2024
- Threat Actor Distributes Python-Based Information Stealer Using a Fake Falcon Sensor Update Lure

July 23, 2024

### SUBSCRIBE

Sign up now to receive the latest notifications and updates from CrowdStrike.

[Sign Up](#)



### See CrowdStrike Falcon® in Action

Detect, prevent, and respond to attacks — even malware-free intrusions — at any stage, with next-generation endpoint protection.

[See Demo](#)