CrowdStrike Falcon Worldwide Outage

July 19, 2024

What it is

CrowdStrike is a network security company. A Falcon Sensor is part of their Cloud-based endpoint protection platform. Think of Endpoint Protection as a firewall on each device that is part of a network. The ‘cloud’ part of it is similar to a conductor in a orchestra, with the endpoints being those playing the instruments, and the instruments are the individual computers/servers.

What caused it

CrowdStrike sent out an update to their software that conflicted with Microsoft Windows, which caused a BSOD (blue screen of death – a ‘crash’ of the software). Following the software crash, the computer gets stuck during reboot and won’t load the operating system, leaving it dead in the water.

How this affects our elections

The idiots that implemented our cloud-based voter registration and poll-book systems have created a HUGE abuse vector in our election ecosystem and I’d be shocked if those election systems weren’t also affected by this. And there is nothing that can prevent their being another accidental (or intentional) abuse! Have you considered that this may just be cover for an election hack just prior to/during an election? It would be perfect

cover.

Maricopa County Voting Locations Impacted – and they aren't alone!

Outages locally have included Maricopa County voting locations, multiple Valley police dispatch centers, several airlines at Phoenix Sky Harbor International Airport and all flights to and from Mesa Gateway Airport.

Gov. Katie Hobbs said on social media that her team is "closely monitoring all services that have been impacted and is working to ensure that we continue delivering the critical services that Arizonans rely on."

> *A worldwide IT outage has impacted some State of Arizona systems and agency operations.*
>
> *My team is closely monitoring all services that have been impacted and is working to ensure that we continue delivering the critical services that Arizonans rely on.*
>
> *As we work to address…*
>
> *— Governor Katie Hobbs (@GovernorHobbs) July 19, 2024*

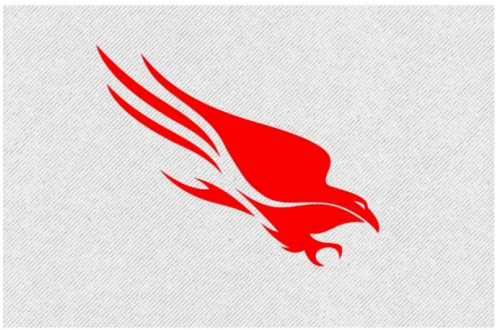
pic.twitter.com/qFLxuYvDHV

— Maricopa County Elections (@MaricopaVote) July 19, 2024

But wait…There’s more! New update from CrowdStrike:

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' 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.

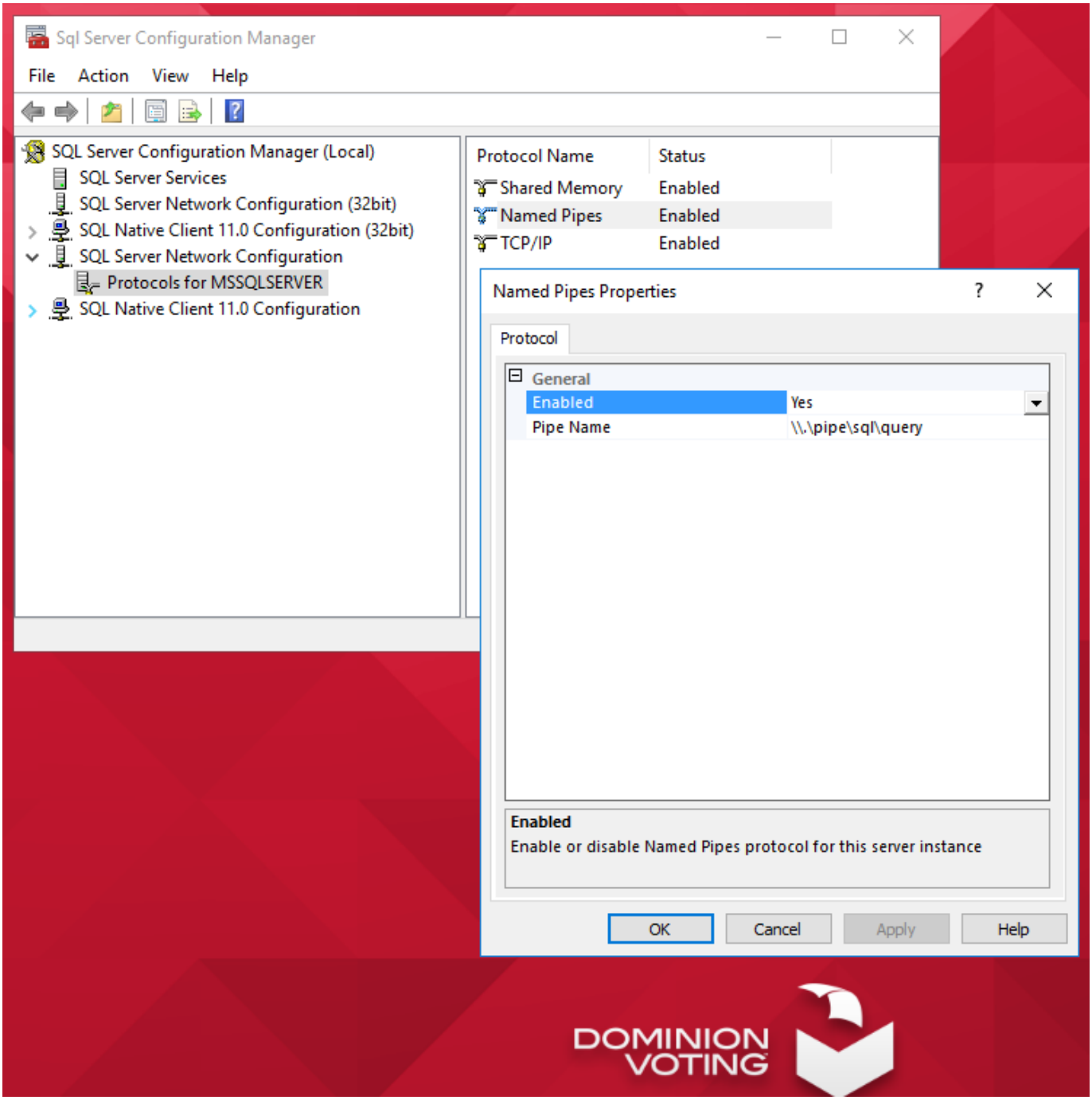
Root Cause Analysis

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.

(Source: https://www.crowdstrike.com/blog/falcon-update-for-windows-hosts-technical-details/)

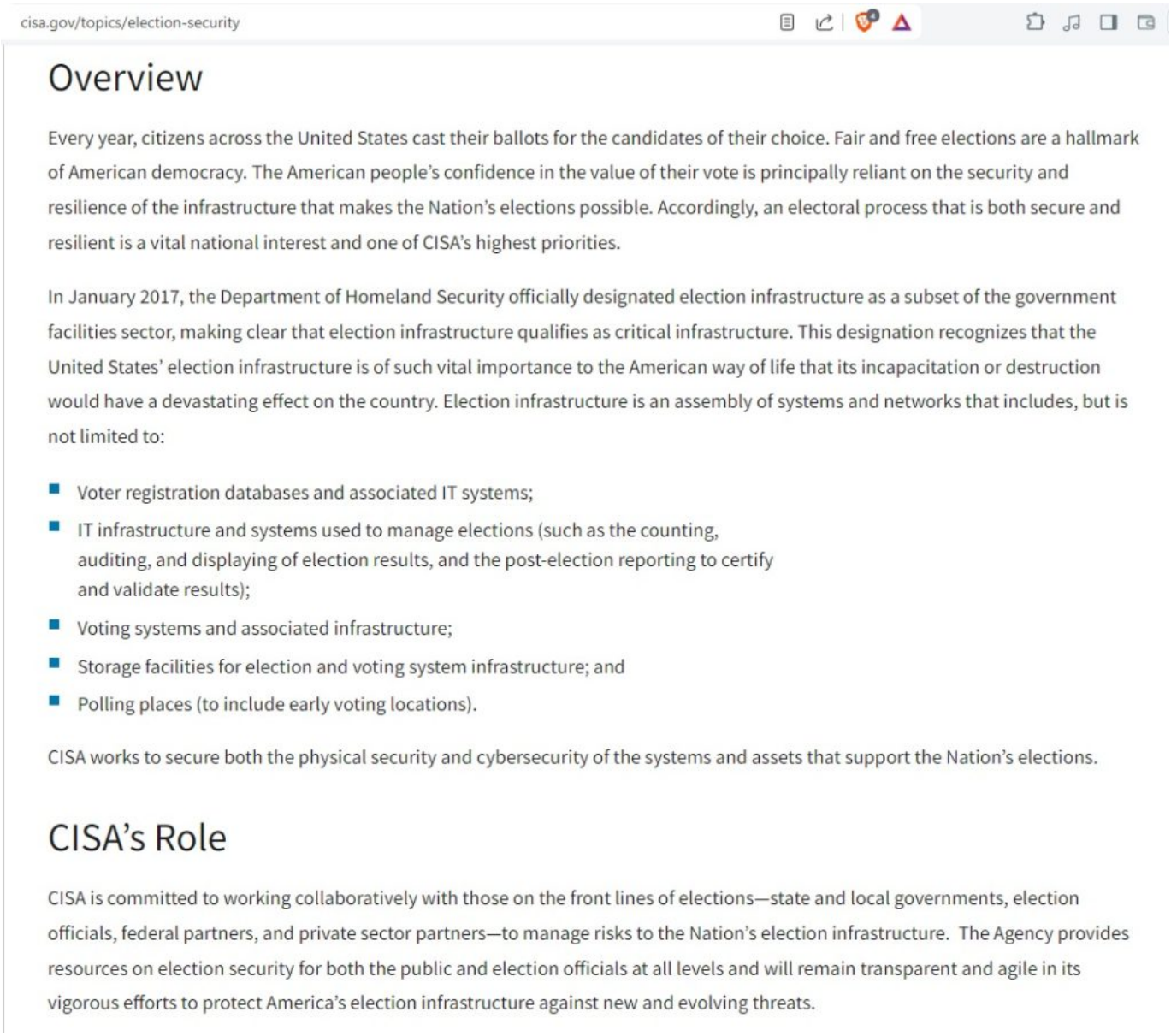
Speaking of Elections…let's not leave out Dominion just yet…

The idiots at Dominion Voting Systems also leave their election management server database server open to Named Pipes (notice the red box above!):



Is this yet another example of their incredible incompetence? Or is it instead, intentional 'incompetence'? And we trust them with WHAT? *(And yes of course, Named-Pipes is not the only problem showing there.)*

According to CISA:



For this system deemed CRITICAL INFRASTRUCTURE, how convenient for Dominion to not even follow standard STIGs. Here's V-79185:

SQL Server must be configured to prohibit or restrict the use of organization-defined protocols as defined in the PPSM CAL and vulnerability assessments.

Overview

Finding ID	Version	Rule ID	IA Controls	Severity
V-79185	SQL6-D0-007600	SV-93891r1_rule		Medium

Description

In order to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable or restrict unused or unnecessary protocols on information systems. Applications are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., email and web services); however, doing so increases risk over limiting the services provided by any one component. To support the requirements and principles of least functionality, the application must support the organizational requirements providing only essential capabilities and limiting the use of protocols to only those required, authorized, and approved to conduct official business or to address authorized quality of life issues. SQL Server using protocols deemed unsafe is open to attack through those protocols. This can allow unauthorized access to the database and through the database to other components of the information system.

STIG	Date
MS SQL Server 2016 Instance Security Technical Implementation Guide	2018-03-09

Details

Check Text (C-78777r1_chk)

To determine the protocol(s) enabled for SQL Server, open SQL Server Configuration Manager. In the left-hand pane, expand SQL Server Network Configuration. Click on the entry for the SQL Server instance under review: "Protocols for ". The right-hand pane displays the protocols enabled for the instance.

If Named Pipes is enabled and not specifically required and authorized, this is a finding.

If any listed protocol is enabled but not authorized, this is a finding.

Fix Text (F-85937r1_fix)

In SQL Server Configuration Manager >> SQL Server Network Configuration >> Protocols, right-click on each listed protocol that is enabled but not authorized and Select "Disable".

Did Dominion do anything else wrong?

Lol…oh boy. This is **barely even the tip of the iceberg**. But in Dominion's defense, it's not just Dominion that's the problem. Every company that electronically centralizes any aspect of our elections creates a superhighway of attack vectors leading into our Nation's entire foundation, our **Election System**. The shear incompetence and inability to protect any system in the industry from abuse is the elephant in the room. When you have a bad actor inside the company, you're done. For instance, look at this **very accurate** quote from an atsec source code review of Dominion that is applicable to ANY system:

> *"Backdoors are extremely hard to find because a seasoned programmer can obfuscate code to look benign. The atsec team would like to stress that, when facing a competent and sufficiently motivated maliciousdeveloper, it is extremely difficult to prove that all backdoors in a system have been identified. The famous Turing award lecture by Ken Thompson in 1984 entitled Reflections on Trusting Trust [TRUST] demonstrated how fundamentally easy it is to undermine all security mechanisms when the developers cannot be trusted. This voting system is no exception."*

Yes, I know CISA claims to secure our systems. Unfortunately, the same types of incompetence in these vendors exist in CISA as well. Not to mention, they are also lying right to our face about many things.

So what is the connection between

CrowdStrike and Dominion?

Well…it is interesting that CrowdStrike is intercepting Named-Pipes and Dominion also left their database connected to Named-Pipes. Coincidence? Possibly. Convenient as yet another possible attack vector? Absolutely!

So what are you trying to say?

Simply put, the people wielding this technology are wholly irresponsible (at best). At worst, what if there are **bad actors** at Dominion? Even worse (if that's even possible), what if there are **bad actors** at CrowdStrike? What do those **bad actors** now have access to? How many millions of computers around the world does CrowdStrike have LOW LEVEL control of? (8.5 Million at the last count according to David Weston, Microsoft VP, Enterprise and OS Security in a blog post Saturday). Who owns CrowdStrike? Who works there? THINK ABOUT ALL THAT…

Our election officials are sitting ducks and in no way knowledgeable enough to secure (nonetheless even understand) this threat landscape. How can any election official claim their system is secure when they don't know it to be such, and they are merely blindly believing what someone they trust tells them? What happens when those that they trust are LYING TO THEM? Our election officials need to accept the reality that is in front of their faces: They cannot control or secure that which they cannot fully see and do not fully understand. The solution is simple…boot all the electronic systems out of our elections and go back to a simple system with a much smaller and controllable threat model, then use technology to add transparency instead of obscurity.

How to fix this current CrowdStrike issue:

The affected file in the update is a particular ‘driver’ that was updated. A ‘driver’ is a program that runs on the computer that performs a task. This driver is the Falcon driver. To repair it, the affected ‘driver’ must be removed in order to allow the operating system to boot up, then the new fixed version of the driver must be installed. The huge complication here is that the driver must be removed MANUALLY. A further complication is for servers that have encrypted hard drives because extra steps must be performed to decrypt the hard drive in order for the repair to be implemented. For companies that didn’t follow best-practices on their encryption passwords, their systems will be permanently locked out and unrecoverable.

Details on repair

The morning of 2024-07-19, a content update was sent to some CrowdStrike Falcon clients on Windows devices which resulted in “Blue Screen” errors for those devices. If you have a Windows device stuck on a blue screen at boot, this issue is almost certainly the cause.

The fix for this issue requires booting the Windows device into Safe Mode or Recovery Mode and deleting a file. Instructions for doing this are below. This post and these instructions may be updated as the situation develops.

FIXING THE WINDOWS DEVICE PROBLEM

Direct link to CrowdStrike instructions: https://www.crowdstrike.com/blog/statement-on-falcon-content-update-for-windows-hosts/

If you are affected by this, we happen to know someone VERY good with solving these types of issues! Contact Mark Cook here.

Workaround Steps for individual hosts:

- Reboot the host to give it an opportunity to download the reverted channel file. If the host crashes again, then:
    - Boot Windows into Safe Mode or the Windows Recovery Environment
        - NOTE: Putting the host on a wired network (as opposed to WiFi) and using Safe Mode with Networking can help remediation. ***(** NOTE: This is the same type of backdoor that many of our electronic voting systems including electronic poll books have)***
    - Navigate to the %WINDIR%\System32\drivers\CrowdStrike directory
    - Locate the file matching “C-00000291*.sys”, and delete it.
    - Boot the host normally.

Workaround Steps for public cloud or similar environment including virtual:

Option 1:

- □□□□□□□Detach the operating system disk volume from the impacted virtual server
- Create a snapshot or backup of the disk volume before proceeding further as a precaution against unintended

changes ***(** NOTE: This type of backup is essentially same thing that Clerk Tina Peters had done to her election system before the SoS and Dominion showed up to remove the QR code feature, that they later attacked her for!)***

- Attach/mount the volume to to a new virtual server
- Navigate to the %WINDIR%\System32\drivers\CrowdStrike directory
- Locate the file matching “C-00000291*.sys”, and delete it.
- Detach the volume from the new virtual server
- Reattach the fixed volume to the impacted virtual server

Option 2:

- □□□□□□□Roll back to a snapshot before 0409 UTC.

AWS-specific documentation:

- To attach an EBS volume to an instance
- Detach an Amazon EBS volume from an instance
    - Note: Use a different OS version for the VirtualMachine used as the recovery VM to the Virtual Machine you are trying to recover.

Azure environments:

- Please see this Microsoft article

User Access to Recovery Key in the

Workspace ONE Portal

When this setting is enabled, users can retrieve the BitLocker Recovery Key from the Workspace ONE portal without the need to contact the HelpDesk for assistance. To turn on the recovery key in the Workspace ONE portal, follow the next steps. Please see this Omnissa article for more information.

Bitlocker recovery-related KBs:

- BitLocker recovery in Microsoft Azure (pdf) or login to view in support portal.
- BitLocker recovery in Microsoft environments using SCCM (pdf) or login to view in support portal.
- BitLocker recovery in Microsoft environments using Active Directory and GPOs (pdf) or login to view in support portal.
- BitLocker recovery in Microsoft environments using Ivanti Endpoint Manager (pdf) or login to view in support portal.