Incident Report: CrowdStrike Software Update Issues

Incident Overview :-

Date of Incident :- *July 19, 2024*

Affected Systems :- *Windows 10 and Windows 11*

Cause :- *Bug in a CrowdStrike software update*

Details of the Incident :-

On July 19, 2024, a critical software update from CrowdStrike's Falcon agents was released, which contained a defect that led to widespread system crashes across numerous Windows devices. Users reported encountering a "blue screen of death" (BSOD) error, rendering their systems inoperable. This incident caused significant disruptions in various industries, particularly in healthcare and transportation, where timely access to systems is crucial.

Incident Timeline

1) February 2024: A new feature was added to the CrowdStrike Falcon sensor to enhance visibility into potential attack techniques.

2) March 5, 2024: The first Rapid Response Content for Channel File 291 was released after a successful stress test.

3) April 2024: Three additional Rapid Response updates were deployed, performing as expected.

4) July 19, 2024: A problematic update was delivered, leading to a system crash due to a mismatch in expected input fields.

Specifics of the Crash

The BSOD errors were characterized by various stop codes, indicating different underlying issues, but all were linked to the faulty update. Many organizations experienced operational downtime, leading to delays in services and potential data loss.

Impact of the Incident

Operational Downtime :- Numerous organizations relying on Windows-based systems faced significant operational challenges, with some unable to access critical applications. This downtime affected productivity and service delivery.

Wider Service Disruptions :- Microsoft cloud services, including Azure and Office 365, were temporarily affected due to the reliance on CrowdStrike for security, leading to a cascade of outages that impacted users globally. This resulted in a loss of access to essential cloud-based applications and services.

Financial Implications :- Organizations began assessing the financial impact of the downtime, with estimates suggesting millions in lost revenue and increased operational costs. The incident prompted many companies to review their disaster recovery and business continuity plans.

What services were affected?

Microsoft estimated that approximately 8.5 million Windows devices were directly affected by the CrowdStrike logic error flaw. That's less than 1% of Microsoft's global Windows install base.

Airlines and airports :- The outage grounded thousands of flights worldwide, leading to significant delays and cancellations of more than 10,000 flights around the world. In the United States, affected airlines included Delta, United and

American Airlines. These airlines were forced to cancel hundreds of flights until systems were restored. Globally, multiple airlines and airports were affected, including KLM, Porter Airlines, Toronto Pearson International Airport, Zurich Airport and Amsterdam Schiphol Airport.

Public transit :- Public transit in multiple cities was affected, including Chicago, Cincinnati, Minneapolis, New York City and Washington, D.C.

Healthcare :- Hospitals and healthcare clinics around the world faced significant disruptions in appointment systems, leading to delays and cancellations. Some states also reported 911 emergency services being affected, including Alaska, Indiana and New Hampshire.

Media and broadcasting :- Multiple media and broadcast outlets around the world, including British broadcaster Sky News, were taken off the air by the outage.

CrowdStrike outage explained

Summary :- A CrowdStrike update caused a massive IT outage, crashing millions of Windows systems. Critical services and business operations were disrupted, revealing tech reliance risks.

What might be considered the largest IT outage in history was triggered by a botched software update from security vendor CrowdStrike, affecting millions of Windows systems around the world. Insurers estimate the outage will cost U.S. Fortune 500 companies $5.4 billion.

The outage occurred July 19, 2024, with millions of Windows systems failing and showing the infamous blue screen of death (BSOD).

CrowdStrike :- the company at the core of the outage -- is an endpoint security vendor whose primary technology is the Falcon platform, which helps protect

systems against potential threats in a bid to minimize cybersecurity risks.

In many respects, the outage was a real manifestation of fears that computing users had at the end of the last century with the Y2K bug. With Y2K, the fear was that a bug in software systems would trigger widespread technology failures. While the CrowdStrike failure was not Y2K, it was a software issue that did, in fact, trigger massive disruption on a scale that has not been seen before.

What caused the outage?

1) The CrowdStrike Falcon platform is widely used by organizations of all sizes across many industries. It is the pervasiveness of CrowdStrike's technology and its integration into so many mission-critical operations and industries that amplified the effect.

2)The outage was not a Microsoft Windows flaw directly, but rather a flaw in CrowdStrike Falcon that triggered the issue.

3) Falcon hooks into the Microsoft Windows OS as a Windows kernel process. The process has high privileges, giving Falcon the ability to monitor operations in real time across the OS. There was a logic flaw in Falcon sensor version 7.11 and above, causing it to crash. Due to CrowdStrike Falcon's tight integration into the Microsoft Windows kernel, it resulted in a Windows system crash and BSOD.

4) The flaw in CrowdStrike Falcon was inside of a sensor configuration update. The sensor is regularly updated -- sometimes multiple times daily -- to provide users with mitigation and threat protection.

5) The flawed update was contained in a file that CrowdStrike refers to as "channel files," which specifically provide configuration updates for behavioral protections. Channel file 291 is an update that was supposed to help improve how Falcon evaluates named pipe execution on Microsoft Windows. Named pipes are a common type of communication mechanism for interprocess communications on

Microsoft Windows.

6) With channel file 291, CrowdStrike inadvertently introduced a logic error, causing the Falcon sensor to crash and, subsequently, Windows systems in which it was integrated.

7) The flaw isn't in all versions of channel file 291. The problematic version is channel file 291 (C-00000291*.sys) with timestamp 2024-07-19 0409 UTC. Channel file 291 timestamped 2024-07-19 0527 UTC or later does not have the logic flaw. By that time, CrowdStrike had noticed its error and reverted the change. But, for many of its users, that reversion came too late as they had already updated, leading to BSOD and inoperable systems.

8) In terms of how the logic error was introduced into the Falcon sensor, the issue was a failure in the CrowdStrike development process. On July 24, 2024, the company issued a preliminary Post Incident Review (PIR). According to the PIR, there was a flaw in CrowdStrike's Content Validator component, used to check the integrity of rapid response content update. That flaw enabled the faulty version of channel file 291 to pass validation, even though it had an error.

9) On Aug. 6, CrowdStrike provided even more details on how the flaw was introduced, with a 12-page root cause analysis report. The report explained that part of the root cause was a mismatch between the number of input fields in the IPC (Inter-Process Communication) Template Type used for the channel file 291 update and the actual inputs provided by the sensor code. The IPC Template Type defined 21 input fields, but the sensor code only provided 20. A runtime array bounds check was missing in the Content Interpreter, and the Content Validator contained a logic error. The conditions that led to those errors were both patched by CrowdStrike after July 19, 2024. Bounds checking came into the system on July 25, 2024, while a patch that validates the number of actual inputs went into production July 27, 2024.

How CrowdStrike aims to prevent future incidents

1) On Sept. 23, 2024, CrowdStrike testified in a U.S. House of Representatives hearing held by the House Subcommittee on Cybersecurity and Infrastructure Protection.

2) During the hearing, Adam Meyers, senior vice president of counter adversary operations at CrowdStrike, apologized to Congress for the outage. Meyers clarified the outage was not due to a cyberattack, but rather a result of a rapid response content update aimed at addressing new threats.

3) During his testimony, Meyers detailed how CrowdStrike has changed its content update procedures to prevent similar incidents in the future:

4) Updates are now treated like code updates, with internal testing and phased implementation.

A new "system of concentric rings" approach for rolling out updates has been implemented.

Customers can now choose their level of update adoption: early adopter, general availability or opt-out/delay.

Investigation and Analysis

Initial Findings

CrowdStrike's internal investigation revealed that a testing tool failed to validate the update properly, allowing a defective version to be distributed. The incident was characterized by Event ID 41 in Windows logs, indicating unexpected shutdowns and system failures. This failure to validate the update before deployment highlighted significant gaps in the quality assurance process.

Remediation Efforts

CrowdStrike's engineering team worked swiftly to identify the bug and issued a clean update to rectify the issue within hours of the incident being reported. Users were advised to boot their systems into Safe Mode to remove problematic files from the CrowdStrike directory, specifically targeting files named C-00000291*.sys.

Steps to Resolve the Issue :-

Boot Windows into Safe Mode or the Windows Recovery Environment.

Navigate to the following directory:

%WINDIR%\System32\drivers\CrowdStrike

Delete any files matching the naming pattern:

C-00000291*.sys

1) Reboot the system normally to restore functionality.

2)Monitor system performance post-reboot to ensure stability.

Recommendations for Users

Immediate Actions:

1)Follow the outlined steps to resolve the BSOD issue promptly.

2) Contact IT support if administrative access is required to perform the fix.

Long-term Solutions :-

Regular Backups :- Implement regular backup solutions to prevent data loss during such incidents. This includes both on-site and off-site backups to ensure data

integrity.

Thorough Testing :- Ensure that all software updates undergo rigorous testing before deployment to avoid similar issues in the future. This should include both automated and manual testing processes.

Incident Response Training :- Provide training for IT staff on incident response protocols to enhance preparedness for future disruptions. Regular drills and simulations can help improve response times and effectiveness.

Conclusion :-

The CrowdStrike update incident on July 19, 2024, highlights the critical importance of rigorous software testing and effective incident response strategies. Organizations must prioritize system monitoring, employee training, and robust backup solutions to mitigate the impact of future disruptions and ensure operational continuity. This incident serves as a reminder of the potential risks associated with software updates and the need for proactive measures to safeguard against them.