TABLE OF CONTENTS

WHEN IT'S NOT THE NETWORK: AN RDP INVESTIGATION THAT LED ELSEWHERE 3
FIXING CROWDSTRIKE ISSUE ON WINDOWS 5
THE HIDDEN DANGERS IN YOUR EMAIL: FILE TYPES TO AVOID FOR CYBERSECURITY 6

SECURITY



WHEN IT’S NOT THE NETWORK: AN RDP INVESTIGATION THAT LED ELSEWHERE

Author(s): Louis Ouellet

In a recent deployment, I was asked to investigate unstable Remote Desktop (RDP) sessions to a remote server accessed over a site-to-site VPN.

At first, the explanation sounded simple: the VPN was unstable. Users were being disconnected, the target server was remote, and all the symptoms seemed to point in the same direction.

On paper, the environment was straightforward:

- Local network: `192.168.115.0/24`

- Remote network: `192.168.201.0/24`
- Original VPN: IPsec
- Temporary replacement VPN: WireGuard
- Target server: `192.168.201.100`
- Multiple users connecting via RDP

But as is often the case in infrastructure work, the first explanation turned out to be the most convenient one — not the most accurate.

> This is one of those cases where everything looks like a network issue — until you start proving what is, and is not, actually failing.

Read more

2026/03/22 20:36 · Louis Ouellet
general, blog, rdp, network, wireguard, investigation, security, windows, linux



FIXING CROWDSTRIKE ISSUE ON WINDOWS

Author(s): Louis Ouellet

Recently, there was a significant issue involving CrowdStrike and Microsoft Windows. On July 19, 2024, CrowdStrike released a routine configuration update for their Falcon sensor software, which led to unexpected system crashes and blue screens of death (BSOD) on Windows systems. The update caused a logic error that corrupted essential system files, triggering widespread outages across various sectors, including healthcare, finance, and critical infrastructure.

Approximately 8.5 million Windows devices were affected, representing less than 1% of all Windows machines globally. The issue primarily impacted systems running the Falcon sensor for Windows version 7.11 and above that were online between 04:09 UTC and 05:27 UTC on the day of the update. The problem was particularly severe for devices with Windows BitLocker encryption enabled, as recovery required an encryption key often stored on servers that were also affected.

To mitigate the issue, users were advised to boot into Safe Mode or the Windows Recovery Environment and delete specific corrupted files from the CrowdStrike directory. CrowdStrike has since rolled back the problematic update and provided manual remediation steps to help affected users restore their systems. They are also conducting a thorough root cause analysis to prevent similar incidents in the future.

Read more

2024/10/29 20:37 · Louis Ouellet
windows, security, cyber-security, crowdstrike, outage, kernel



THE HIDDEN DANGERS IN YOUR EMAIL: FILE TYPES TO AVOID FOR CYBERSECURITY

Author(s): Louis Ouellet

Emails are a common medium for communication, but they can also be a gateway for cyber threats. In this post, we delve into the types of email attachments that pose risks and why it's crucial to stay vigilant. Understanding these risks is key to protecting your personal and organizational data from malicious attacks.

Read more

2023/12/13 10:55
cyber-security, security, email safety, malware, phishing

From:
https://laswitchtech.com/ - **LaswitchTech**

Permanent link:
https://laswitchtech.com/en/blog/security/index

Last update: **2026/03/24 12:42**