Microsoft and CrowdStrike Are Fixing a Big Mess

Yusuf

2024-07-27T20:57:13Z

Hey guys,

So, Microsoft has been pretty busy helping CrowdStrike clean up a big mess from a week ago. It all started when an update from CrowdStrike went haywire and knocked out 8.5 million PCs. Now, Microsoft's pushing for some changes to Windows, hinting that they want to make Windows more resilient and maybe even stop security vendors like CrowdStrike from accessing the Windows kernel.

CrowdStrike blamed a bug in their testing software for the bad update. Since their software runs at the kernel level (the core part of the OS with full access to system memory and hardware), any issues can cause big problems like the infamous Blue Screen of Death. Their Falcon software uses a special driver to run deeper than most apps to catch threats across a Windows system.

Microsoft has tried to block third parties from kernel access before, back with Windows Vista in 2006, but faced a lot of pushback from cybersecurity vendors and EU regulators. Apple, on the other hand, locked down macOS in 2020, blocking developers from kernel access.

Now, Microsoft seems ready to talk about restricting kernel-level access in Windows again. John Cable, the VP of program management for Windows servicing and delivery, said in a blog post that Windows needs to focus on end-to-end resilience and called for better cooperation with partners to boost security. He droped a few hints about future changes, like a new VBS enclaves feature that doesn't need kernel mode drivers to be tamper-resistant and mentioned Microsoft's Azure Attestation service as an example of recent security improvements.

Cable said these features use modern Zero Trust approaches and show what can be done without relying on kernel access. He also mentioned that Microsoft will keep working on these capabilities, hardening the platform, and improving Windows' resilience with help from the security comunity.

This could spark a new debate about Windows kernel access, even though Microsoft might not be able to lock down Windows like Apple did with macOS because of regulatory reasons. Cloudflare's CEO has already warned about the potential downsides of Microsoft tightening Windows access, so it's something they'll have to think about carefully.

On the other side, CrowdStrike said that almost all Microsoft Windows sensors are back online after their faulty update caused chaos worldwide. They said over 97% of Windows sensors were operational again by Wednesday evening, after their July 19 update crashed millions of Windows-based devices and frooze corporate networks.

Microsoft estimates that the error affected 8.5 million Windows devices and could cost Fortune 500 companies over $5 billion in losses. CrowdStrike's CEO, George Kurtz, appologized on LinkedIn, promising to restore systems as quickly as possible and learn from the mistake.

The global outage showed just how fragile interconnected IT systems can be. McKinsey & Company pointed out that it highlights the trade-offs IT teams have to make between updating to protect against cyberattacks and managing changes that can introduce instability.

Delta Air Lines, one of the companies hit hard by the outage, said they had to cancel thousands of flights but things are back to normal now.

Hope this keeps you in the loop!

Catch you later!

source: https://www.theverge.com/2024/7/26/24206719/microsoft-windows-changes-crowdstrike-kernel-driver

https://www.cbsnews.com/news/crowdstrike-outage-microsoft-windows-restored/