TechTarget | ComputerWeekly.com E-guide

CW+ Content

CrowdStrike outage explained

What happened and what can we learn?

In this e-guide

In this E-guide:

A botched content update released by CrowdStrike in July 2024 led to a massive IT outage affecting about 8.5 million Windows systems worldwide.

This incident, considered one of the largest of its kind, impacted various industries and services, including airlines, hospitals, and government websites, leading to disruptions and significant financial losses.

CrowdStrike identified and reverted the error, but the outage persisted as affected computers required manual fixes. More importantly, it highlighted the potential risks associated with automatic software updates and the interconnected nature of modern IT systems.

In this e-guide, learn more about how the outage occurred, its impact on organisations around the globe, and what you can do to mitigate the risks of similar incidents in future.

CrowdStrike update chaos explained: What you need to know

Alex Scroxton, Security Editor

On Friday 19 July 2024, the UK awoke to news of a fast-spreading IT outage, seemingly global in its nature, affecting hundreds – if not thousands – of organisations.

The disruption began in the early hours of Friday morning in Australia, before spreading quickly across Asia, Europe and the Americas, with the travel industry among the most widely affected.

The outage was quickly tracked to cyber security firm CrowdStrike, which is already engaged in incident response amid the chaos. Keep on top of this developing incident over the coming days and weeks with our Essential Guide.

What does CrowdStrike do?

CrowdStrike is one of the world’s most prominent cyber security companies, with thousands of customers all over the world. Based in Texas, it employs more than 8,000 people and books about $3bn in revenues per annum. It has been around since 2011.

The organisation bills itself thus: “CrowdStrike has redefined security with the world’s most advanced cloud-native platform that protects and enables the people, processes and technologies that drive modern enterprise. CrowdStrike secures the most critical areas of risk – endpoints and cloud workloads, identity, and data – to keep customers ahead of today’s adversaries and stop breaches.”

CrowdStrike will be unfamiliar to most people not steeped in the technology industry, although Formula 1 fans will be aware of it thanks to its headline sponsorship of the Mercedes AMG Petronas team – its branding appears on the halo safety device and is clearly seen on onboard footage from Lewis Hamilton’s car.

Security practitioners will know CrowdStrike from its frequent contributions to major incident investigations, including the Sony Pictures hack, the WannaCry crisis, and the 2016 hack of the Democratic National Committee by Russia.

What happened during the CrowdStrike outage?

The disruption at first manifested in the form of the infamous blue screen of death – which signals a fatal system error – on Windows PCs.

Given the disruption appeared to be a Microsoft problem to begin with, it was Redmond that first responded, confirming just before 8am BST that it was investigating problems affecting cloud services in the US.

It quickly became apparent that the issue was not down to Microsoft itself, but rather a faulty channel file rolled out to CrowdStrike’s Falcon sensor product.

Falcon is a solution designed to prevent cyber attacks by unifying next-gen antivirus, endpoint detection and response (EDR), threat intelligence and threat hunting, and security hygiene. This is all managed and delivered through a lightweight, cloud-delivered and -managed sensor.

CrowdStrike's preliminary investigation has now identified the source of the outage as a cloud-delivered, rapid response update to the Falcon sensor. CrowdStrike uses these updates to identify new indicators of threat actor behaviour, and improve its detection and prevention capabilities.

However, in this instance, a template containing "problematic" content data leading to the out-of-bound memory condition which was to trigger Microsoft systems to crash, was cleared for delivery thanks to a bug in CrowdStrike's automated content validator tool.

The errors cumulatively caused what is known as a boot loop. This is a situation that occurs when a Windows device restarts without warning during its startup process – meaning the machine cannot finish a complete and stable boot cycle and, therefore, won’t turn on. Such issues will in general occur either due to inadequate testing across various desktop and server environments, or due to a lack of proper sandboxing and rollback mechanisms for updates that involve a kernel-level interaction.

At the time of writing, more information about the precise nature of the incident continues to emerge but the full facts have not been fully established, and an investigation will likely take some time.

Is there a cyber security threat from the CrowdStrike outage?

Though similar in its effect and origins to a supply chain attack, it is important to note that the CrowdStrike outage is not a cyber security incident and nobody is known to be under attack as a result of it.

However, as it affects a cyber security product threat actors will take advantage of the downtime caused and any gaps in coverage arising. This has already started to happen, within hours of the incident unfolding CrowdStrike itself said it identified a malicious ZIP archive circulating which purported to contain a utility to help automate recovery, but was in fact a so-called remote access Trojan (RAT).

Multiple national cyber security agencies, including the UK's National Cyber Security Centre (NCSC) and partners in Australia, Singapore and the US, have also issued cyber alerts and advisories in the wake of the outage.

The coming days and weeks will see threat actors exploiting the incident in phishing and social engineering attacks as they attempt to lure new victims.

Potential lures could include offers of technical support or bogus CrowdStrike updates, and the consequences could include data exfiltration, ransomware deployment and extortion.

Researchers at Akamai say they have identified well over 180 malicious domains exploiting CrowdStrike's misfortune circulating, many of them incorporating keywords likely to be used by people searching for more information. Some of these websites are known to be linked to large-scale malicious phishing operations, and similar to email phishing lures, purport to offer information on technical support, fixes and updates, and even potential class action lawsuits.

Security and IT leaders and admins would be well-advised to communicate the potential follow-on dangers to their users. The most effective thing anybody can do is to only trust information and updates that come directly from CrowdStrike via its dedicated incident hub.

Who was affected by the CrowdStrike outage?

According to Microsoft, the incident affected approximately 8.5 million Windows devices worldwide, making up less than 1% of the entire estate. Redmond said that while this was a tiny number, all things considered, the widespread economic and societal impacts of the incident reflected the use of CrowdStrike by many organisations that run critical public-facing services.

The full number of organisations affected by the outage is not known for now. However, those that are known to have, or have confirmed they have, experienced some impact include:

- Airlines including American Airlines, Delta, KLM, Lufthansa, Ryanair, SAS and United;
- Airports including Gatwick, Luton, Stansted and Schiphol;
- Financial organisations including the London Stock Exchange, Lloyds Bank and Visa;
- Healthcare including most GP surgeries and many independent pharmacies;
- Media organisations including MTV, VH1, Sky and some BBC channels;
- Retailers, leisure and hospitality organisations including Gail's Bakery, Ladbrokes, Morrisons, Tesco and Sainsbury's;
- Sporting bodies including F1 teams Aston Martin Aramco, Mercedes AMG Petronas and Williams Racing, which were preparing to compete at the Hungarian Grand Prix at the time, and the Paris 2024 Organising Committee for the Olympic and Paralympic Games, which begin in a few days;
- Train operating companies (TOCs) such as Avanti West Coast, Merseyrail, Southern and Transport for Wales.

What is CrowdStrike saying about the outage?

In an initial statement, CrowdStrike CEO George Kurtz said: "CrowdStrike is actively working with customers impacted by a defect found in a single content update for Windows hosts. Mac and Linux hosts are not impacted. This is not a security incident or cyber attack.

“The issue has been identified, isolated and a fix has been deployed. We refer customers to the support portal for the latest updates and will continue to provide complete and continuous updates on our website.

“We further recommend organisations ensure they’re communicating with CrowdStrike representatives through official channels. Our team is fully mobilised to ensure the security and stability of CrowdStrike customers.”

In a breakfast TV interview with NBC in the US on 19 July, Kurtz added: “We’re deeply sorry for the impact that we’ve caused to customers, to travellers, to anyone affected by this, including our companies.”

He later added: “Nothing is more important to me than the trust and confidence that our customers and partners have put into CrowdStrike. As we resolve this incident, you have my commitment to provide full transparency on how this occurred and steps we’re taking to prevent anything like this from happening again.”

What is CrowdStrike doing about it?

Beyond rolling back the tainted update, which was done within the space of just over an hour and a quarter, CrowdStrike has since set out a number of changes to be made to ensure this doesn't happen again.

CrowdStrike has now set out an extensive preliminary plan designed to keep such an incident from occurring again.

This includes improving the resiliency of rapid response updates through enhanced developer testing, update and rollback testing, stress testing, fuzzing and fault injection, stability testing, and content interface testing. It will also add better validation checks to its content validator system, and enhance some other components of its setup with improved error handling capabilities.

Going forward, updates made under the rapid response programme will be staggered, rolling out bit by bit across the installed base of Falcon sensors, beginning with what is known as a canary deployment. Party During this process, enhanced monitoring will be conducted on sensor and system performance, and as a last resort, customers will be given the ability to control the delivery of such updates, which will also be clearly set-out to them with release notes.

In this e-guide

As of the weekend of 27 - 28 July, CrowdStrike leadership was reporting that 97% of the affected Falcon sensors had been successfully recovered. The company also told TechTarget Editorial that it was working towards rolling out a backend fix for the logic error that caused its automated validator to miss the dodgy code. This is expected to be made in the coming days.

What has been Microsoft's response?

Microsoft has been working extensively alongside CrowdStrike to automate work on developing and pushing a fix, and in the wake of the outages hundreds of its engineers and software experts were deployed to work directly with customers on service restoration.

Microsoft has also been collaborating with cloud providers such as Google Cloud and Amazon Web Services (AWS) to share awareness on the impacts seen, and better inform ongoing dialogue with customers and CrowdStrike itself.

Subsequently, Redmond has fallen back on an EU anti-competition ruling from 2009 as a line of defence. This ruling holds that Microsoft must ensure the interoperability of third-party products with relevant software products on an equal basis. Ultimately, this means Microsoft appears to believe it was forced to allow CrowdStrike too deep into its core operating system.

Can I fix the CrowdStrike problem myself?

CrowdStrike has rolled back the changes to the affected product automatically, but hosts may continue to crash or be unable to stay online to receive the remedial update.

The short answer to the question is yes, but unfortunately, such issues can be daunting to fix, requiring IT teams to put in a lot of work. It may be days, or even longer, before all the affected devices can be reached.

System administrators are advised to take the following steps:

1. Boot Windows into safe mode, or the Windows Recovery Environment;
2. Navigate to C:\Windows\System32\drivers\CrowdStrike directory;
3. Locate the file matching “C-00000291*.sys”. Delete this file;
4. Boot normally.

CrowdStrike customers can access more information by logging into its support portal.

How can I avoid similar problems in the future?

Security firms such as CrowdStrike are under a great deal of pressure when it comes to product development and updates, which must be done frequently as

In this e-guide

they strive to keep their customers protected from new zero-days, ransomware and the like.

This pressure also trickles down to customers themselves, who will understandably often want to take advantage of settings to allow their security tools to update automatically.

To avoid falling victim to this kind of problem going forward, IT teams should consider taking a phased approach to software updates – particularly if they pertain to security solutions – and test them in a sandbox environment, or on a limited set of devices, prior to full deployment.

It is also wise to have some level of system redundancy built in to properly isolate and manage fault domains, particularly when running critical infrastructure. IT teams should also attend to IT asset management and software asset management, and establish strong disaster recovery and business continuity planning as a priority, and these should of course be tested regularly.

Those organisations that were unaffected should view the situation as a wake-up-call, instead of a lucky escape.

Next Article

CrowdStrike says most Falcon sensors now up and running

Alex Scroxton, Security Editor

The majority of CrowdStrike Falcon sensors affected by a botched rapid response update were back up and running prior to the weekend of 27 and 28 July, as efforts to remediate the 19 July incident that caused more than eight million Windows machines to crash continue.

Writing on LinkedIn on 26 July, CrowdStrike CEO George Kurtz, who has been communicating information about the incident at a steady clip since it first unfolded, said that as of Thursday 25 July "over 97%" of Windows sensors were back online.

"This progress is thanks to the tireless efforts of our customers, partners, and the dedication of our team at CrowdStrike. However, we understand our work is not yet complete, and we remain committed to restoring every impacted system," said Kurtz.

"To our customers still affected, please know we will not rest until we achieve full recovery. At CrowdStrike, our mission is to earn your trust by safeguarding your operations. I am deeply sorry for the disruption this outage has caused and personally apologise to everyone impacted. While I can't promise perfection, I can promise a response that is focused, effective, and with a sense of urgency."

Kurtz said the remedial efforts had been greatly helped thanks to the use of automated recovery techniques and by mobilising all possible resources to support affected customers. He reiterated CrowdStrike's commitment to its core mission – to stop breaches – but with a new focus on customer controls and resilience, as detailed in the firm's preliminary incident report last week.

Fixed update set for implementation soon

Meanwhile, CrowdStrike confirmed to Computer Weekly's sister title TechTarget Security prior to the weekend that the logic error in its validator tool that caused the chaos was definitely fixed, and intensive testing is now underway before the update can be pushed to live on its backend systems, set for the coming days.

The tainted update was part of a rapid response roll-out normally used by CrowdStrike to enhance the dynamic protection mechanisms of its Falcon platform – that is to say, it was designed to identify new cyber security issues and help customers mitigate them.

The company performs such updates all the time, but on this occasion, some problematic content in a channel file made it past the beady eyes of CrowdStrike's automated content validator. The two issues combined led to an out-of-bound memory condition, which triggered an exception overwhelming the Windows operating system and causing vulnerable devices to fail and crash, resulting in the infamous blue screen of death.

CrowdStrike is attempting to make sure the issue cannot replicate in future by improving the resilience of its rapid response updates through improved testing at multiple levels, and adding refreshed validation checks to the automated content validator tool that let it down.

It also now plans to roll out rapid response updates on a staggered basis, deploying them across the Falcon sensor base more slowly and making use of "canary" deployments designed to highlight any major issues before they spread.

This will see sensor and system performance receive enhanced monitoring, and at some point, CrowdStrike customers are to be given more options to manage rapid response updates themselves.

Real-life impacts

Meanwhile, real-world impacts continue to be felt from the outage, which notably caused airlines all over the world to delay, reschedule and cancel flights.

Among the stories to have emerged is that of an 83-year-old man who became the subject of a search operation by authorities in the US. Patrick Bailey, who was scheduled to fly home from Florida to California on 19 July, was put up in a local hotel when his flight was cancelled.

Although Bailey checked out the following morning, he accidentally left his mobile phone in his room and went missing for several days. Bailey eventually turned up in California on 28 July, having instead decided to take a long-distance Greyhound bus across the US.

Next Article

Why did CrowdStrike cause the Windows Blue Screen?

Cliff Saran, Managing Editor

David William Plummer, a former Microsoft software engineer who developed Windows Task Manager, has posted a video describing how the CrowdStrike update could have caused Windows to halt.

He described CrowdStrike Falcon as anti-malware for Windows servers, which “proactively detects new attacks” and analyses application behaviour. To do this, CrowdStrike needs to run as a kernel device driver.

Kernel device drivers usually provide a way to abstract hardware, such as graphics cards, from applications. When they run, they generally have full access to the computer and operating system and, in operating system terminology, they are said to run at “Ring Zero”. This is different to application code, which users run in the operating system’s user space known as “Ring One”.

The difference, as Plummer notes, is that when a user application crashes, nothing else on the computer should be affected. However, a fault in code running at Ring Zero is considered so serious that the operating system immediately halts, which, in Windows results in the so-called Blue Screen of Death.

"Even though there's no hardware device that it's really talking to, by writing the code as a device driver, CrowdStrike lives down in the kernel Ring Zero and has complete and unfettered access to the system data structures and the services that CrowdStrike believes it needs to do its job," said Plummer.

Certified device drivers

Plummer noted that Microsoft, and likely also CrowdStrike, are aware of the stakes when software is running code in kernel mode, adding: "That's why Microsoft offers the WHQL [Windows Hardware Quality Labs] certification."

According to Plummer, the certification involves device driver software providers to test their code on various platforms and system configurations. The code is then signed digitally by Microsoft, which certifies that it is compatible with the Windows operating system. Plummer said the certifications process means that Windows users can be reasonably confident that the driver software is robust and trustworthy.

Certification is too slow to ensure anti-malware protection such as CrowdStrike is released as software updates every time there is a new threat. Plummer believes it is more likely that CrowdStrike will often release a definition file that is processed by its Windows kernel driver. This gets around the WHQL device driver certification process and means users have access to the latest protection.

"You can already perhaps see the problem," he added. "Let's speculate for a moment that the CrowdStrike dynamic definition file is not merely a malware definition but a complete program written in pseudocode that the driver can then execute."

He said this would allow the device driver from CrowdStrike to execute the definition file as code running within the Windows kernel at Ring Zero even though the update itself has never been signed. "Executive p-code [pseudocode] in the kernel is risky at best and, at worst, is asking for trouble," said Plummer.

By looking at crash dumps posted on X (formerly Twitter), Plummer said that a "null pointer reference" caused an empty file containing zeros to be uploaded by the CrowdStrike device driver, rather than the actual pseudocode.

"We don't know how or why this happened, but what we know is that the CrowdStrike driver that handles and processes these updates is not very resilient and appears to have inadequate error-checking and parameter validation," he added.

These are needed to ensure that data values required by the software are valid and good. If they are not, the error should not cause the entire system to crash, Plummer said.

While it is often possible to restart Windows from the last known “good state”, which can remove rogue kernel drivers that prevent the operating system from booting up, Plummer said the situation was made worse by the fact that CrowdStrike is marked as a boot-start driver, which means it is needed for Windows to start up correctly.

While it is too early to understand how to ensure this never happens again, it is clear that there are serious limitations in Microsoft’s WHQL certification that allowed CrowdStrike to install an anti-malware update that had such a devastating impact across the Windows community.

Next Article

CrowdStrike update snafu affected 8.5 million Windows devices

Aaron Tan, Executive Editor, APAC

About 8.5 million Windows devices worldwide were affected by the botched CrowdStrike update, making up less than 1% of all Windows machines, according to Microsoft.

In a blog post, Microsoft said while the percentage was small, the broad economic and societal impacts of the incident reflect the use of CrowdStrike by enterprises that run many critical services.

On 19 July 2024, a content update that included malware signatures rolled out to users of the CrowdStrike Falcon endpoint protection service led to outages after affected Windows machines started experiencing a Blue Screen of Death (BSOD) error.

In Asia-Pacific, the affected organisations included Malaysia’s AirAsia, Australia’s Coles and Woolworths, India’s PhonePe and Tata Starbucks, as well as Airports of Thailand, among others.

“We recognise the disruption this problem has caused for businesses and in the daily routines of many individuals,” Microsoft said. “Our focus is providing customers with technical guidance and support to safely bring disrupted systems back online."

The software giant said it is engaging with CrowdStrike to automate the work on developing a fix and has deployed hundreds of Microsoft engineers and experts to work directly with customers to restore services.

It is also collaborating with other cloud providers including Google Cloud and Amazon Web Services to share awareness on the state of impact they are seeing across the industry and inform ongoing conversations with CrowdStrike and customers.

In a message posted on X earlier today, CrowdStrike said of the approximately 8.5 million Windows devices that were impacted, a significant number are back online and operational.

CrowdStrike has also been working with customers to test a new technique to speed up remediation of impacted systems and is in the process of operationalising an opt-in to the technique. "We're making progress by the minute," it added.

In the aftermath of the outage, some national cyber security agencies in the region have warned of an increase in related scams.

On 20 July 2024, Michelle McGuinness, Australia's National Cyber Security Coordinator, said there were increasing reports of scammers attempting to exploit recovery efforts.

"As systems are being restored, I urge Australian businesses and members of the community to be vigilant. Do not engage with suspicious websites, emails, texts and phone calls," she said.

Singapore's Cyber Security Agency also warned of an ongoing phishing campaign targeting CrowdStrike users, with threat actors leveraging the outage as "lure themes" to send phishing emails posing as CrowdStrike support to customers and impersonate CrowdStrike staff in phone calls.

The emails could also be purportedly from independent researchers, claiming to have evidence that the technical issue is linked to a cyber attack and offering remediation insights.

Next Article

Fortune 500 stands to lose $5bn plus from CrowdStrike incident

Alex Scroxton, Security Editor

The total direct financial loss faced by Fortune 500 companies as a result of the 19 July Microsoft-CrowdStrike outage has been set at approximately $5.4bn (£4.18bn), at an average weighted loss of $44m per organisation, rising to close to $150m for the most heavily affected, such as airlines.

This is according to cloud monitoring, modelling and insurance services provider Parametrix, which said that for many Fortune 500 organisations, the impact would be heightened because their large risk retentions and low policy limits relative to potential losses means the portion covered under cyber insurance policies is likely to amount to no more than 10% to 20% of the total loss.

Parametrix analysis found the largest direct financial loss is likely to fall on those in the healthcare sector – down $1.94bn cumulatively, followed by banking – down $1.15bn. This accounts for 57% of the total loss, but only 20% of Fortune 500 revenues due to the uneven impact of the event.

For example, the firm’s analysts said that manufacturing, the largest Fortune 500 segment by revenue, will suffer a relatively trivial loss of just $36m compared with its annual revenue of $3.4tn across 130 organisations, while the six airlines represented on the list will be out $860m against total revenues of $187.1bn.

Parametrix said about a quarter of Fortune 500 organisations were impacted in the incident, caused by a coding error in a CrowdStrike update that threw computers into a boot loop and brought systems crashing down. This includes all six of the Fortune 500 airlines and 43% of retailers. Meanwhile, three-quarters of health and banking firms will suffer direct costs.

“Our analysis of the CrowdStrike outage shows not only the possible extent of a systemic cyber loss event, but also its boundaries,” said Jonatan Hatzor, co-founder and CEO of Parametrix.

“It tells us more about the ways that insurers and reinsurers can diversify their cyber risk portfolios to minimise the potential impacts of systemic cyber risk. However, our analysis does not show the whole diversification picture. A cyber insurer focused on very large companies will certainly suffer a much greater CrowdStrike loss relative to premium than one with a large SME book.”

Beyond financial losses, the impact of the downtime on critical services resulted in a highly visible cascade of operational delays affecting Fortune 500 companies and downstream entities.
Parametrix said it was likely that in terms of recovering systems, those industries that still rely heavily on physical computers will be the ones to experience longer recovery times – a point in favour of cloud services, it noted.

It said the overall impact of the outage was made more distinct due to CrowdStrike's deployment both on-premise and in cloud environments.

Based on this, the firm forecast, cyber insurers should not necessarily rely solely on the event for modelling future cloud-based failures, but might try to better manage systemic outage risks through diversifying across industry sectors, service providers and company sizes.

"Prevention is important, but risk carriers have limited control over event occurrences and service-provider practices," he said.

"The industry should focus on controllable areas, like mapping and managing aggregation risk. By understanding these points, we can evaluate key exposures, and mitigate both malicious and non-malicious threats. This proactive approach enables better underwriting decisions, and effective risk-transfer solutions to manage systemic risk."

Single point of failure

More broadly, Hatzor echoed concerns already shared by other observers in the wake of the global outage – namely the prevalence of tightly bundled technology services that risk creating single points of failure.

"In today's digital landscape, many businesses rely heavily on integrated systems and services, which, while efficient, can also leave them vulnerable," he said. "When a critical component within a tightly bundled solution experiences downtime or fails, it can trigger a cascade of disruptions throughout the entire system.

"This interconnectedness means that a failure in one area can lead to significant operational disruptions, affecting everything from customer service to data management and financial transactions."

Hatzor raised further concerns that both regulators and cyber insurers are not really prepared to address the complexities and risks of such systems. As so often happens, he noted, the rapid evolution of technology has outpaced the development of regulatory frameworks and risk assessment models, which leaves businesses exposed to gaps in insurance coverage or regulatory support when the worst comes to pass.

"This lack of preparedness can exacerbate the impact … leaving companies more vulnerable to prolonged downtime and financial losses," he said.

Next Article

CrowdStrike outage underscores software testing dilemmas

Beth Pariseau, Senior News Writer

Endpoint security vendor CrowdStrike pledged to improve its software testing after a flawed content update caused a massive Windows systems outage last week. But avoiding future incidents might not be that simple, according to IT experts.

CrowdStrike issued a preliminary incident review this week detailing how a software bug caused a failure in the content validation tool it uses to look for errors such as the one that sent some 8.5 million Windows machines into a reboot loop last week. The company also clarified that the update was to configuration data within what it calls a Rapid Response Content template rather than to its main codebase or OS kernel drivers.

Rapid Response Content is meant to monitor systems for emerging cybersecurity threats "at operational speed," according to the CrowdStrike report. This type of file is more frequently updated than CrowdStrike's core application and had been subject to a less-extensive testing process. Following last week's incident, however, the company pledged to apply the same software testing procedures, including canary deployments, to Rapid Response Content.

In one software engineer's view, CrowdStrike is rightly answering for "doing lots of stuff it shouldn't," including less-thorough testing on Rapid Release Content updates that still had direct access to the Windows OS.

"Even testing for one minute would have discovered these issues," said Kyler Middleton, senior principal software engineer at healthcare tech company Veradigm. "In my mind, that one minute of testing would have been acceptable."

In general, software testing and test coverage is lacking in many corners of the market. For example, a Federal Communications Commission report this week found that an AT&T mobile network outage in February was caused by a network configuration update that had not followed the telco's own internal testing procedures.

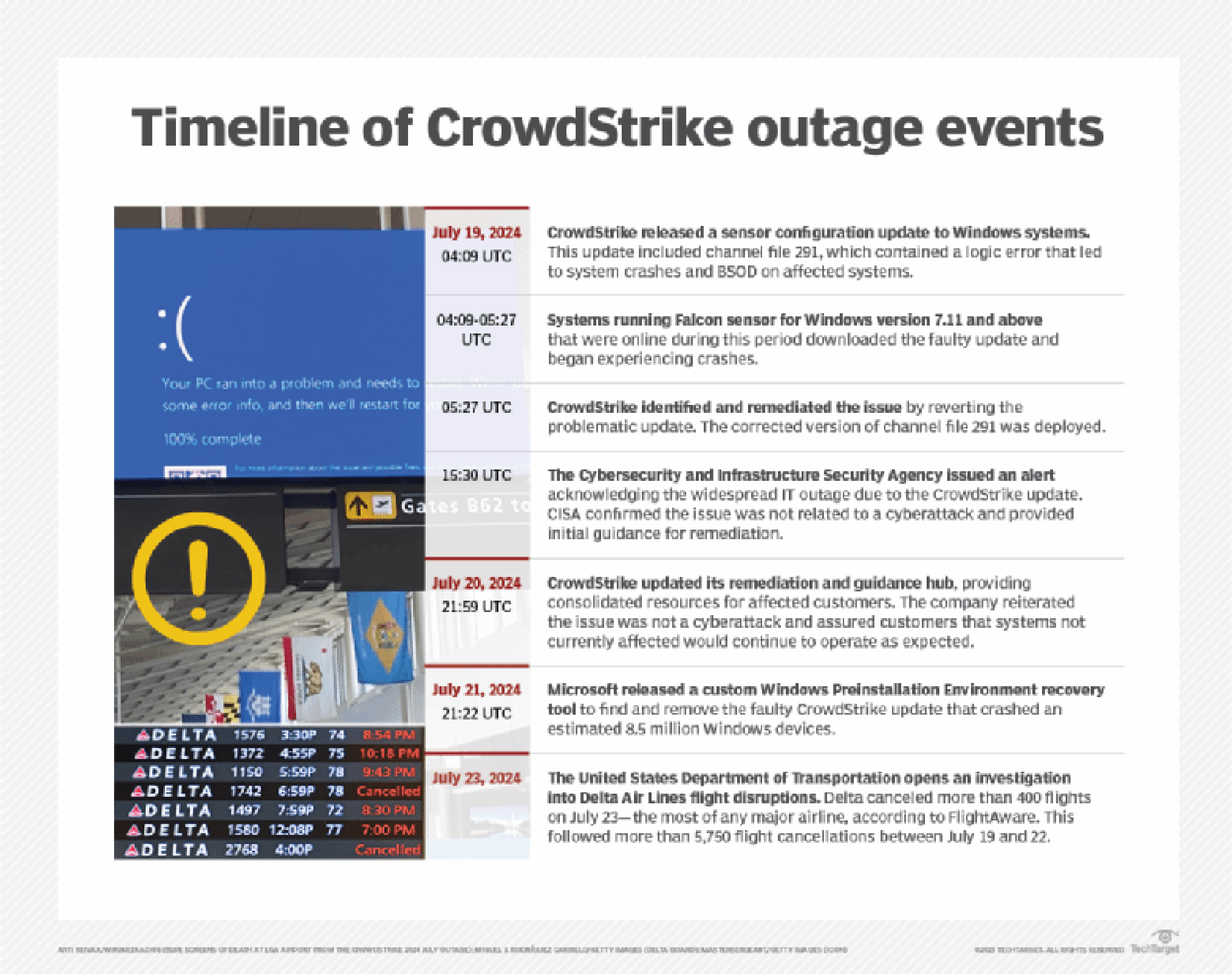
This wasn't an isolated incident for IT, according to IDC data. The analyst firm's June 2024 "DevOps Practices, Perceptions, and Tooling" survey found that just 44% of 300 respondents' software quality tests were automated. Additionally, 27.3% chose testing and QA as one of the top two bottlenecks in their DevOps pipelines.

"Testing continues to be a significant point of friction [in application development]," IDC analyst Katie Norton said. "Software quality governance requires automation with agile, continuous quality initiatives in the face of constrained QA staff and increasing software complexity."

Software testing, both for security and quality, appears to be among the most promising uses for generative AI in other IDC surveys, Norton said.

"I am hopeful that the next few years will see improvements in these statistics," she said. "However, AI can't fix the lack of or failure to follow policy and procedures."

In this e-guide


:(
Your PC ran into a problem and needs to
some error info, and then we'll restart for
100% complete
Gates B62 to
DELTA 1576 3:30P 74 8:54 PM
DELTA 1372 4:55P 75 10:18 PM
DELTA 1150 5:59P 78 9:43 PM
DELTA 1742 6:59P 78 Cancelled
DELTA 1497 7:59P 72 8:30 PM
DELTA 1580 12:08P 77 7:00 PM
DELTA 2768 4:00P Cancelled

Timeline of CrowdStrike outage events

July 19, 2024 04:09 UTC	**CrowdStrike released a sensor configuration update to Windows systems.** This update included channel file 291, which contained a logic error that led to system crashes and BSOD on affected systems.
04:09-05:27 UTC	**Systems running Falcon sensor for Windows version 7.11 and above** that were online during this period downloaded the faulty update and began experiencing crashes.
05:27 UTC	**CrowdStrike identified and remediated the issue** by reverting the problematic update. The corrected version of channel file 291 was deployed.
15:30 UTC	**The Cybersecurity and Infrastructure Security Agency issued an alert** acknowledging the widespread IT outage due to the CrowdStrike update. CISA confirmed the issue was not related to a cyberattack and provided initial guidance for remediation.
July 20, 2024 21:59 UTC	**CrowdStrike updated its remediation and guidance hub**, providing consolidated resources for affected customers. The company reiterated the issue was not a cyberattack and assured customers that systems not currently affected would continue to operate as expected.
July 21, 2024 21:22 UTC	**Microsoft released a custom Windows Preinstallation Environment recovery tool** to find and remove the faulty CrowdStrike update that crashed an estimated 8.5 million Windows devices.
July 23, 2024	**The United States Department of Transportation opens an investigation into Delta Air Lines flight disruptions.** Delta canceled more than 400 flights on July 23—the most of any major airline, according to FlightAware. This followed more than 5,750 flight cancellations between July 19 and 22.

ANTI SEVAA/WIKIMEDIA (BLUE SCREENS OF DEATH AT LGA AIRPORT FROM THE CROWDSTRIKE 2024 JULY OUTAGE); MIGUEL J. RODRÍGUEZ CARRILLO/GETTY IMAGES (DELTA BOARDS); MASTERSERGEANT/GETTY IMAGES (CORP)

Balancing velocity, stability and security

However, Middleton and other industry observers acknowledged that the CrowdStrike outage wasn't simply caused by lax software testing processes. Instead, it's an example of the complex set of factors software developers must weigh when testing releases.

The CrowdStrike flaw was caused by multiple layers of bugs. That includes a content validator software testing tool that should have detected the flaw in the Rapid Release Content configuration template -- an indirect method that, in theory, poses less of a risk of causing a system crash than updates to system files themselves, said Gabe Knuth, an analyst at TechTarget's Enterprise Strategy Group.

"This is a challenge in fully automated systems because they, too, rely on software to progress releases from development through delivery," Knuth said. "If there's a bug in the software somewhere in that CI/CD pipeline … it can lead to a situation like this. So to discover the testing bug in an automated way, you'd have to test the tests. But that's software, too, so you'd have to test the test that tests the tests and so on."

How extensive software testing should be depends on a risk assessment that encompasses not only the stability of systems but also how quickly they can be updated to mitigate rapidly emerging security threats.

In this e-guide

"What's worse?" Knuth said. "A bug that crashes millions of endpoints and causes global disruption while it's fixed or a damaging vulnerability that results in lost intellectual property, private information, state secrets, etc.?"

As painful as a Windows outage that grounded airline flights and affected hospital systems was, for many companies, that kind of security compromise would be worse, Middleton said.

"In the end, companies would rather risk an availability failure from a bad update [to] their security tooling than risk a confidentiality failure from malware compromising their hosts," she said. "On the outside, as consumers, we see it as about the same -- the services we use aren't available. But from the inside, it's totally different."

While compromised service availability affects the bottom line to a small degree, according to Middleton, malware could leak data that causes a company to close due to legal fees or causes so much damage to a company's reputation that it loses customers.

"Companies would much rather be shut down by a bad update than malware," Middleton said. More extensive software testing "does come with risks. These update files are composed to quickly respond to emerging malware threats, and any delay, even one minute, could possibly leave the door open for a sensitive enterprise server to be infected."

IT pros call for canary deployments and more

In response to the outage, CrowdStrike will perform incrementally phased rollouts of changes, or canary updates, with Rapid Release Content files the same way it does with less frequent app updates, according to the company's preliminary post-incident report.

For some organizations, this will offer some reassurance that a flawed update won't hit every customer machine all at once.

"I'm incredibly surprised, even though they call it 'Rapid Response,' that [CrowdStrike] doesn't have some phased approach that allows them to check in on the health of the endpoints that have been deployed," said Andy Domeier, senior director of technology at SPS Commerce, a Minneapolis-based communications network for supply chain and logistics businesses. "Even with some logical order of customer criticality, they could have circuit breakers to stop a deployment early that they see causes health issues. For example, don't [update] airlines until your confidence level is higher from seeing the health of endpoints from other customers."

Other software engineers said canary deployments would be a good step. However, they said CrowdStrike should rethink its application architecture more broadly so that rapidly updated files are separated from the operating system kernel by an abstraction layer, such as a management controller, hypervisor or eBPF program.

> *Companies would much rather be shut down by a bad update than malware.*
> *Senior principal software engineer, Veradigm*
> *Kyler Middleton*

"It is absolutely irresponsible to auto-deploy a kernel module update globally without a health-mediated process or, at least, a recovery path at a lower level of the control plane," said David Strauss, co-founder and CTO at WebOps service provider Pantheon. "Something that remains functional even if the OS deployed on top crashes."

Customers that run such relatively high-octane malware detection software on relatively noncritical machines also bear some responsibility for the impact of the CrowdStrike outage, Strauss added.

"The use of CrowdStrike on things like airline gate terminals is absurd to me," he said. "Machines like that are single-purpose and should be secured using restricted privileges … and integrity validation. … The only place where it makes sense to watch for malware is when you can't do those two things. Even then, app stores, signed releases and OS-enforced sandboxing are the modern approaches to handling that -- much more than scanning agents that run on end-user computer devices."

Next Article

CrowdStrike chaos shows risks of concentrated 'big IT'

Alex Scroxton, Security Editor

The global Microsoft outage caused by a botched update from security firm CrowdStrike has highlighted the dangerous business continuity risk arising from concentrating so much of the world's technology infrastructure in the hands of a very small number of businesses, experts are warning.

The outage, which began late on Thursday 18 July 2024 before spreading worldwide and hitting the headlines early in the morning of Friday 19 July, saw a bugged CrowdStrike update make it through quality control to worldwide deployment. When it hit computers, it threw them into what is known as a boot loop, causing them to crash on startup and display the infamous blue screen of death.

It's estimated that it affected only about 8.5 million machines, which is a fraction of the global total, but with many of those belonging to public-facing organisations, pictures of bricked display screens in locations such as airports, railway stations and shops swiftly went viral.

Citing data from a study his firm published in May 2024, SecurityScorecard CEO and co-founder Aleksandr Yampolskiy revealed that IT products and services made by just 150 companies account for 90% of the global attack service, while 62% of the global attack surface is concentrated in the line-ups of just 15 tech firms – including Microsoft.

Ranked on Security Scorecard's proprietary rating system, the original study claimed that those 15 organisations all had below-average cyber security risk ratings, and given ransomware gangs – and others – are known to systematically target third-party vulnerabilities at scale, this should be a significant worry for IT teams.

Yampolskiy described the state of much of global IT as a "precarious house perched on a cliff's edge", and said that in concentrating mission-critical services to a few big companies, businesses have created a single point of failure.

"When I used to work at Goldman Sachs, the policy was to get tools from multiple vendors," he said. "This way, if one firewall goes down by one vendor, you have another vendor who may be more resilient. [Friday's] global outage is a reminder of the fragility and systemic 'nth-party' concentration risk of the technology that runs everyday life: airlines, banks, telecoms, stock exchanges and more.

Grasping the chaos

Yampolskiy said the survey's findings emphasised how a significant proportion of the global external attack surface is controlled by a small number of organisations, and that we are only just beginning to grasp the chaos – thrown into sharp relief thanks to events at CrowdStrike – that this could cause.

He argued that the CrowdStrike incident aptly demonstrated how knowing your supply chain (KYSC) was becoming an increasingly important part of operational resilience, adding that IT teams needed to better understand the dependencies in their business and those of their tech suppliers, and that such knowledge is critical to responding to outages effectively, whether they result from malicious cyber attacks, human error or something else.

"Understanding and managing your supply chain is critical in mitigating these risks," said Yampolskiy. "By proactively identifying dependencies and potential vulnerabilities within your ecosystem, you can strengthen your organisation's resilience against such disruptive events.

"An outage is just another form of a security incident," he said. "Antifragility in these situations comes from not putting all your eggs in one basket. You need to have diverse systems, know where your single points of failure are, and proactively stress-test through tabletop exercises and simulations of outages. Consider the 'chaos monkey' concept, where you deliberately break your systems – for example, shut down your database or make your firewall malfunction to see how your computers react.”

Next Article

CrowdStrike chaos: Enterprises urged to take protective action in wake of botched software update

Caroline Donnelly, Senior Editor, UK

Microsoft users across the globe should review the state of their infrastructure security setups in the wake of the botched CrowdStrike software update that took millions of Windows devices across the world offline on Friday 19 July 2024.

As stated in a blog post, authored by Microsoft's vice-president of enterprise and operating system security, David Weston, on 20 July 2024, "this was not a Microsoft incident" but one that "impacts our ecosystem" and had disrupted the businesses and "the daily routines of many individuals".

According to Microsoft's calculations, around 8.5 million Windows devices, which equates to less than 1% of the global total of Windows machines in use, were affected by the incident.

And while that percentage might seem small in the grand scheme of things, Owen Sayers – an independent security consultant with more than 20 years' experience advising public sector and policing clients on how to secure their systems – said the numbers involved are “terrifying” when coupled with information gleaned from CrowdStrike’s own incident reporting blog.

As confirmed by its “*Technical details: Falcon content update for Windows hosts*” blog, the corrupt software update that caused the Friday 19 July outage was only online for 78 minutes before it was taken down and replaced with a fixed version. “It affected less than 1% of global Windows devices in that time – that’s impressive,” said Sayers, but it also has worrying implications for the state of our global IT systems.

Knowing that a bug in a third-party security product could wreak so much havoc in such a short amount of time could give nation-state hackers some food for thought on how to wage their next wave of attacks.

“The Chinese and Russians now know how to bring down global IT systems – just find a security product used by your target, and modify that code,” said Sayers. “And there is a damn good chance it’ll wipe them out within an hour and a half.”

Travel disruption

The CrowdStrike incident caused travel disruption at major airports and train stations, as well as affecting the day-to-day operations of GP surgeries, retailers and other businesses running Microsoft technologies. And, in some cases, its effects are still being felt days later.

“Folks like to think about outages like this in terms of full-day terms or even a weekend [of disruption being caused] due to the ongoing effect, but when you distil the cause down to lasting less than an hour and a half, it gets more impactful,” said Sayers.

“This time the error was in a third-party product that only a very small number of organisations use, but look at the scale and the spread of the damage.”

With this in mind, what would happen if a third-party product with higher rates of take-up within the Microsoft user community suffered a similar botched software update? Or, if Microsoft rolled out an operating system or service pack update to its user base that similarly risked bricking its customers’ devices?

It might sound like a scaremongering question to ask, but Eric Grenier, director analyst at market watcher Gartner for Technical Professionals, told Computer Weekly that any IT supplier who “hooks into” the Windows kernel in a similar way to CrowdStrike could suffer a similar fate if they were to release a defective update.

“You can even go a step higher and say that every vendor who releases an update has the potential to release a ‘bad patch’,” he said.

For this reason, Grenier said the situation should give the entire software industry pause for thought to ensure they do not become the next CrowdStrike. “This is a good time for everyone in the software industry to review their quality assurance processes as well as their software update testing processes, and fortify them the best they can,” he added.

User protection

End-user organisations whose Windows systems were unaffected by the Friday 19 July update should view the situation as a wake-up call, rather than a lucky escape, said Rich Gibbons, head of IT asset management market development and engagement at independent software licensing advisory Synyega.

“If your organisation avoided this issue, [it is] likely because they are not a CrowdStrike customer, so take this as a wake-up call,” he told Computer Weekly.

“Unfortunately, all organisations are open to the risk of their business being negatively impacted by a third-party supplier making a huge error. Accepting that risk and having a strong disaster recovery and business continuity planning [strategy] is key and must be a priority for every business.”

Having robust IT asset management (ITAM) and software asset management (SAM) systems in place is also a must, continued Gibbons. “Knowing what software and hardware you have, where it is, [as well as its] support and end of life status, last patch and update time and data are also key having an effective disaster recovery and business continuity plan, whether resources are on-premise or in the cloud within hybrid environments," he said.

As Gartner's Grenier points out, having a disaster recovery and business continuity strategy in place is one thing, but enterprises must also be sure to test them regularly.
"This is not the last time a vendor will release a 'bad patch', so to mitigate risk, client organisations will need to review [these] strategies and actually test them to be sure they meet the standard they are looking for in terms of 'time-to-recovery'," he said.

"Organisations should also take the opportunity to review which applications in their environment are on 'auto-update' and gauge the potential fall-out from a 'bad update'."

That's not to say Grenier is advocating that there should be a blanket switch-off of the "auto-update" functionality across enterprises around the world to mitigate the risk of another CrowdStrike occurring.

"That should be determined by the organisation's risk acceptance level and whether they can patch applications themselves," he said. "Enterprises should have a documented inventory of which applications are set to 'auto-update', whether or not you can turn ‘auto-update’ off and know what the impact could be if a bad update or patch is delivered for each application set to ‘auto-update’.

“If they choose to manually update applications they will also need to build processes and workflows around testing updates for each application,” said Grenier.

Next Article

In this e-guide

CrowdStrike outage shows business continuity still a must

Tim McCarthy, News Writer

A faulty update issued by cybersecurity vendor CrowdStrike brought numerous companies to their knees July 19, exposing critical vulnerabilities in disaster recovery plans.

IT analysts said the interconnected nature of SaaS, cloud services and modern applications contributed to the massive IT outage, which triggered a looping blue screen of death on devices running the Windows OS with CrowdStrike's threat detection software.

> *If there's a silver lining to this [event], it'll get the attention of the not-technically-minded members of your board.*
> *Vice president of research, Enterprise Management Associates*
> *Chris Steffen*

This connectivity in software and hardware is needed for organizations to operate and meet consumer demands, but they must also consider traditional business continuity plans and recovery, analysts said.

The advent of cloud services and automation has led to a lax attitude toward patching, updates and system access, according to Chris Steffen, vice president of research at Enterprise Management Associates. Customers that rely on vendor automation for updates should plan for worst-case scenarios and exert more control, both in business contracts and when rolling out software updates, he added.

"I don't know how seriously people are taking disaster recovery anymore because [with the cloud] that's someone else's problem," Steffen said. "If there's a silver lining to this [event], it'll get the attention of the not-technically-minded members of your board."

Automated automation

CrowdStrike has issued guidance on how to undo the error, which has affected an estimated 8.5 million devices, and now offers an automated remediation capability.

Those tools might come as cold comfort for industries such as airlines, which suffered massive service disruptions and grounded flights for days due to the thousands of Windows endpoints that accepted the faulty update.

Companies that use security and threat detection software from vendors such as CrowdStrike are still better off automatically accepting updates despite this setback, Steffen said, as they patch for new vulnerabilities and cause little issue.

"We've been screaming for years about the necessity of having automatic updates," Steffen said. "Most of the world is starting to get that message, and then it happens that an automatic update destroys the world."

Automating updates is also needed to ensure that software continues to function across the entire organization's IT infrastructure, according to Jerome Wendt, president and founder of Data Center Intelligence Group.

Organizations adding software and complexity to their IT environments should understand a map of their resources, how each component of software or hardware could affect these services and the blast radius in the case of failure, he said.

"We have to live in the real world," Wendt said. "There's going to be interdependencies. … I don't put that on CrowdStrike. I put that on the organizations. That's on you to know what's going on."

Road to recovery

Ideally, a recovery plan for a software issue should include automated rollback capabilities, according to Keith Townsend, chief technology adviser at the Futurum Group.

"This is definitely one of those things you can prepare for," Townsend said. "A lot of this is standard stuff [for recovery]."

These rollbacks should separate the application data from the OS, enabling a more granular recovery without affecting data, he said.

In this case, deployment of automated remediation tools was further complicated by many of these systems running the CrowdStrike software on Windows desktops typically managed by employees, according to Steven McDowell, founder and chief analyst at NAND Research.

As remote or hybrid work becomes increasingly standardized, IT teams will need to make sure they have recovery options available for endpoints like these alongside servers and other hardware, since getting access on demand could be difficult, McDowell said.

"We're realizing the desktop is critical infrastructure," he said.

Organizations have spent the past decade considering backup and disaster recovery from the perspective of cyberattacks through ransomware, but traditional disaster and outages are still an ongoing threat, according to Mike Matchett, founder and president of Small World Big Data.

Developing a business continuity strategy might require additional hardware resources, a costly addition for some organizations. It might also mean finding ways to keep the business operational even if it comes down to using pen and paper. It's a hard lesson IT has learned again and again throughout history.

"It's maybe time to take a deeper look at your business continuity plan over disaster recovery," Matchett said. "If you're going to talk recovery, it's a multi-day process."

Next Article

Computer Weekly and TechTarget coverage of the CrowdStrike incident

- 19 July 2024: An update to CrowdStrike's Falcon service has led to many Windows users being unable to work this morning. Microsoft 365 is also affected.
- The Emis Web IT system used by more than half of GP practices in the UK is down, following the worldwide Microsoft outage.
- The global outage of Microsoft is rapidly sending shockwaves across all sectors, demonstrating the risk of having a single point of failure.
- A CrowdStrike update with a faulty sensor file has global implications for Windows systems. But competitors need to limit the finger-pointing in case it happens to them.
- As organisations recover from today's outages, the cyber security industry will need to develop new security software evaluation criteria and requirements and learn to parlay risks.
- 22 July: About 8.5 million devices globally were hit by the botched CrowdStrike update, with a significant number now back online and operational.
- The concentration of so much mission-critical technology in the hands of a few large suppliers makes incidents like the Microsoft-CrowdStrike outage all the more dangerous.
- Financially motivated cyber criminals are already conducting opportunistic attacks on organisations that leverage the CrowdStrike incident, and more targeted attacks are sure to follow.

- 23 July: The ‘blue screen of death’ signals a catastrophic Windows failure, which is exactly what many people faced on 19 July 2024 – but why did it happen? One former Microsoft engineer has a theory.
- Disaster recovery has centered on cyberattacks the past few years, but the CrowdStrike outage illustrates why companies can't forget about traditional business continuity.
- 24 July: Enterprises that emerged unscathed from the roll-out of the botched CrowdStrike software update are being urged to view it as a wake-up call rather than a lucky escape.
- The largest global organisations hit by the CrowdStrike - Microsoft incident on 19 July will likely be out of pocket to the tune of billions of dollars.
- CrowdStrike publishes the preliminary findings of what will be a lengthy investigation into the root causes of the failed 19 July update that caused Windows computers to crash all over the world.
- 25 July: Microsoft has pointed the finger at EU reguators, blaming them for a ruling that means it needs to offer third parties like CrowdStrike access to the core Windows OS.
- 26 July: Experts say efforts to avoid incidents such as last week's CrowdStrike outage will face time-honoured tradeoffs between velocity, stability, access and security.
- CrowdStrike customers grappling with blue screens of death from the recent IT outage may be able to sidestep BitLocker encryption schemes and recover their Windows systems.
- 29 July: The vast majority of CrowdStrike Falcon sensors affected by a coding error have now been recovered, with a final resolution expected this week.
- Malicious domains exploiting CrowdStrike’s branding are popping up in the wake of the 19 July outage. Experts share some noteworthy examples, and advice on how to avoid getting caught out.

Getting more CW+ exclusive content

As a CW+ member, you have access to TechTarget's entire portfolio of 120+ websites. CW+ access directs you to members-only content that is guaranteed to save you the time, and ultimately help you to solve your toughest IT challenges more effectively.

Take full advantage of your membership by visiting www.computerweekly.com/eproducts

Images: stock.adobe.com