NZ Incident Response Bulletin

Premium Edition – July 2024 – Issue #66

The NZ Incident Response Bulletin is a monthly high-level executive summary containing some of the most important news articles that have been published on Forensic and Cyber Security matters during the last month. Each Bulletin also includes a section of our own content, based on a trending theme. We'll give you a brief summary of each article, and a link to more information. Why do we publish this bulletin? Because we want to keep you up to date with the latest Forensic and Cyber Security news, so that you aren't caught by surprise – and you'll know about risks and changes before they become problems.

Special Edition – Crowdstrike Global IT Outage Incident

On 19 July 2024, a faulty software update to the CrowdStrike vulnerability scanner Falcon Sensor caused blue screens of death on Microsoft Windows machines, disrupting millions of Windows computers worldwide. Affected machines were forced into a bootloop, making them unusable. The downtime impacted global transportation, banking, media, emergency services and others. In this bulletin, along with our regular content, we summarise the key developments and outline mitigations to respond to this incident, and others that are likely to continue to happen in the future.

The following articles have been published by Crowdstrike:

Statement on Falcon Content Update for Windows Hosts

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 was not a cyberattack.

The issue has been identified, isolated and a fix has been deployed. We are referring customers to the support portal for the latest updates and will continue to provide complete and continuous public updates on our blog. We further recommend organizations ensure they're communicating with CrowdStrike representatives through official channels. Our team is fully mobilized to ensure the security and stability of CrowdStrike customers. We understand the gravity of the situation and are deeply sorry for the inconvenience and disruption. We are working with all impacted customers to ensure that systems are back up and they can deliver the services their customers are counting on. We assure our customers that CrowdStrike is operating normally and this issue does not affect our Falcon platform systems. If your systems are operating normally, there is no impact to their protection if the Falcon sensor is installed.

Below is the latest CrowdStrike Tech Alert with more information about the issue and workaround steps organizations can take. We will continue to provide updates to our community and the industry as they become available.

Details

- Symptoms include hosts experiencing a bugcheck\blue screen error related to the Falcon sensor.
- Windows hosts that have not been impacted do not require any action as the problematic channel file has been reverted.
- Windows hosts that are brought online after 0527 UTC will also not be impacted
- This issue is not impacting Mac- or Linux-based hosts
- Channel file "C-00000291*.sys" with timestamp of 0527 UTC or later is the reverted (good) version.
- Channel file "C-00000291*.sys" with timestamp of 0409 UTC is the problematic version.
    - Note: It is normal for multiple "C-00000291*.sys files to be present in the CrowdStrike directory - as long as one of the files in the folder has a timestamp of 0527 UTC or later, that will be the active content.

Technical Details on Today's Outage

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[1] 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.

[1] https://learn.microsoft.com/en-us/windows/win32/ipc/named-pipes

Falcon Sensor Content Issue from July 19, 2024, Likely Used to Target CrowdStrike Customers

On July 19, 2024, an issue present in a single content update for the CrowdStrike Falcon® sensor impacting Windows operating systems was identified, and a fix was deployed. CrowdStrike Intelligence has monitored for malicious activity leveraging the event as a lure theme and received reports that threat actors are conducting the following activity:

- Sending phishing emails posing as CrowdStrike support to customers
- Impersonating CrowdStrike staff in phone calls
- Posing as independent researchers, claiming to have evidence the technical issue is linked to a cyberattack and offering remediation insights
- Selling scripts purporting to automate recovery from the content update issue

The below provides a list of domains identified on 19 July 2024, that impersonate CrowdStrike’s brand. Some domains in this list are not currently serving malicious content or could be intended to amplify negative sentiment. However, these sites may support future social-engineering operations.

crowdstrike.phpartners[.]org
crowdstrike0day[.]com
crowdstrikebluescreen[.]com
crowdstrike-bsod[.]com
crowdstrikeupdate[.]com
crowdstrikebsod[.]com
www.crowdstrike0day[.]com
www.fix-crowdstrike-bsod[.]com
crowdstrikeoutage[.]info
www.microsoftcrowdstrike[.]com
crowdstrikeodayl[.]com
crowdstrike[.]buzz
www.crowdstriketoken[.]com
www.crowdstrikefix[.]com
fix-crowdstrike-apocalypse[.]com
microsoftcrowdstrike[.]com
crowdstrikedoomsday[.]com
crowdstrikedown[.]com
whatiscrowdstrike[.]com
crowdstrike-helpdesk[.]com
crowdstrikefix[.]com
fix-crowdstrike-bsod[.]com
crowdstrikedown[.]site
crowdstuck[.]org
crowdfalcon-immed-update[.]com
crowdstriketoken[.]com
crowdstrikeclaim[.]com
crowdstrikeblueteam[.]com
crowdstrikefix[.]zip
crowdstrikereport[.]com

News:

A high-level executive summary containing some of the most important news articles that have been published on Forensic and Cyber Security matters during the last month.

New Zealand

New Zealand National Cyber Security Centre (NCSC) statement on global IT outage

An IT outage following an update made by CrowdStrike software has caused significant disruption globally. This update resulted in outages in windows systems. The issue has been identified, isolated and the vendor has released remediation guidance for customers, available via their CrowdStrike Customer Portal which will be updated as the situation evolves. The NCSC encourages New Zealand organisations that have been impacted by this disruption to review the guidance issued by the vendor and act immediately. The NCSC has no information to indicate these issues are related to malicious cyber security activity.

However, there has been an observed increase in phishing referencing this outage as opportunistic malicious cyber actors seek to take advantage of the situation. We encourage organisations and individuals to be alert to this increased activity. Helpful resources to protect against phishing are available here - Know the Risks - Own Your Online

CrowdStrike failure: Kiwis wake after night of chaos following global IT outage

Kiwi supermarkets are open and operating without difficulties this morning after a global IT outage described as the worst in history crippled the globe. In an update issued this morning, Retail NZ said today’s early indications were that retail and payment systems were back up and running. “Supermarkets are opening and are not currently experiencing difficulties with payments and point of sale systems, however as this global issue is now in ‘fix mode’ there is the possibility of further outages,” Retail NZ chief executive Carolyn Young said. “We urge consumers to be patient and if possible to have the ability to pay via cash and/or Eftpos, which was a more stable platform last night due to the agreements amongst banks to be able to transact offline. “This is still a live issue that will continue to develop over the weekend and it emphasises how much we rely on technology and the cloud to enable us to go about our daily activities. While we are a long way from the United States, we are not immune to being impacted by global events such as what we saw on Friday evening.”

CrowdStrike outage: Acting PM David Seymour has 'overwhelming expectation' NZ systems back up and running soon

New Zealand appears to have avoided the worst of the global CrowdStrike IT glitch, says Acting Prime Minister David Seymour. Services globally are slowly recovering from a crippling software update failure deployed on Friday night (NZ time) which took out computer systems belonging to airlines, healthcare providers, retailers, news outlets, broadcasters, financial outlets, infrastructure and transport networks and more.

CrowdStrike, the cybersecurity firm that issued the faulty software update, says the bug is fixed - but it could be some time before all systems are back up and running. Seymour told RNZ on Saturday morning the latest prognosis for New Zealand was "good news. The software fix is in, it's been installed, government departments have not lost any critical services at any time. I've been in touch with the New Zealand Bankers Association - they say it's likely that they're going to be at business as usual with banking today, although they haven't confirmed that with me absolutely.”

He said the National Emergency Management Agency was called in on Friday night just in case the damage to IT systems here was worse. "Earlier in the evening, it wasn't clear if this would be over in a few hours - as thankfully it has been from a software point of view - or whether it was a disruption that might continue for several days. So their job is to check that various government services are able to continue and that people are going to be able to get the necessaries of life. It appears that no critical services that people rely on are in any danger, and the overwhelming expectation is that we will be back to business as usual today."

Australia

Scammers taking advantage of Crowdstrike outage, experts warn

Malicious websites and unofficial code are being used to try and scam people during the Crowdstrike outage, Australia's Cyber Security Centre has warned. ACSC's Australian Signals Directorate, one of Australia's leading spy and counterintelligence agencies, has warned that fake websites and code are being released online, claiming to fix the global technical outage caused by Crowdstrike's software update. The malicious sites are mimicking the Crowdstrike website, providing fake code and instructions.

"ASD's ACSC understands a number of malicious websites and unofficial code are being released claiming to help entities recover from the widespread outages caused by the CrowdStrike technical incident. ASD's ACSC strongly encourages all consumers to source their technical information and updates from official CrowdStrike sources only." The full list of fake websites, identified by Crowdstrike, are listed on the official Crowdstrike website, which can be found here.

World

Cybersecurity and Infrastructure Security Agency - Widespread IT Outage Due to CrowdStrike Update

CISA is aware of the widespread outage affecting Microsoft Windows hosts due to an issue with a recent CrowdStrike update and is working closely with CrowdStrike and federal, state, local, tribal and territorial (SLTT) partners, as well as critical infrastructure and international partners to assess impacts and support remediation efforts. CrowdStrike has confirmed the outage:

- Impacts Windows 10 and later systems.
- Does not impact Mac and Linux hosts.
- Is due to the CrowdStrike Falcon content update and not to malicious cyber activity.

According to CrowdStrike, the issue has been identified, isolated and a fix has been deployed. CrowdStrike customer organizations should reference CrowdStrike guidance and their customer portal to resolve the issue.

Of note, CISA has observed threat actors taking advantage of this incident for phishing and other malicious activity. CISA urges organizations and individuals to remain vigilant and only follow instructions from legitimate sources. CISA recommends organizations to remind their employees to avoid clicking on phishing emails or suspicious links.

- The CrowdStrike guidance is updated with additional guidance regarding impacts to specific environments, e.g., Azure, AWS.
- For additional information:
    - Update from the United Kingdom's National Cyber Security Centre (NCSC-UK)
    - Update from the Australian Cyber Security Centre (ACSC)
    - Update from the Canadian Centre for Cyber Security (CCCS)
- Threat actors continue to use the widespread IT outage for phishing and other malicious activity. CISA urges organizations to ensure they have robust cybersecurity measures to protect their users, assets, and data against this activity.

CISA continues to monitor the situation and will update this Alert to provide continued support.

Statement from Microsoft CEO

Yesterday, CrowdStrike released an update that began impacting IT systems globally. We are aware of this issue and are working closely with CrowdStrike and across the industry to provide customers technical guidance and support to safely bring their systems back online.

Regular News:

OAIC takes civil penalty action against Medibank

The Australian Information Commissioner has filed civil penalty proceedings in the Federal Court against Medibank Private Limited in relation to its October 2022 data breach. The Commissioner alleges that from March 2021 to October 2022, Medibank seriously interfered with the privacy of 9.7 million Australians by failing to take reasonable steps to protect their personal information from misuse and unauthorised access or disclosure in breach of the Privacy Act 1988.

The proceedings follow an investigation initiated by Australian Information Commissioner Angelene Falk after Medibank was the subject of a cyber attack in which one or more threat actors accessed the personal information of millions of current and former customers, which was subsequently released on the dark web. “The release of personal information on the dark web exposed a large number of Australians to the likelihood of serious harm, including potential emotional distress and the material risk of identity theft, extortion and financial crime,” said acting Australian Information Commissioner Elizabeth Tydd.

Medibank’s business as a health insurance services provider centrally involves collecting and holding customers’ personal and sensitive health information. In the financial year ending June 2022, Medibank generated a revenue of $7.1 billion and an annual profit of $560 million. “We allege Medibank failed to take reasonable steps to protect personal information it held given its size, resources, the nature and volume of the sensitive and personal information it handled, and the risk of serious harm for an individual in the case of a breach,” said Commissioner Tydd.

“We consider Medibank’s conduct resulted in a serious interference with the privacy of a very large number of individuals.” Privacy Commissioner Carly Kind said, “Organisations that collect, use and store personal information have a considerable responsibility to ensure that data is held safely and securely. That is particularly the case when it comes to sensitive data. This case should serve as a wakeup call to Australian organisations to invest in their digital defences to meet the challenges of an evolving cyber landscape. Organisations have an ethical as well as legal duty to protect the personal information they are entrusted with and a responsibility to keep it safe.”

MediSecure declares insolvency following massive data breach

Vaughan Strawbridge and Paul Harlond of FTI Consulting were appointed as voluntary administrators on 3 June and as liquidators of operations on 4 June. Control of MediSecure has now passed to the firm. “We recognise the significant concern and the impact of the recent cyber incident. The company has been in contact with the Australian government with respect to providing information in response to that incident,” Strawbridge said in a 5 June statement. “Our role as administrators and liquidators includes investigating the affairs of the company to identify reasons for its failure and to examine options that may be available to recover assets for the benefit of creditors of the companies. “We will be speaking to the Australian government about what they need from the company and the next steps in the response to the cyber incident.” The initial hack was first revealed on 16 May, after the National Cyber Security Coordinator had warned of a “large-scale ransomware data breach incident”. A week later, a hacker by the name of Ansgar claimed responsibility for the hack and posted several files of sample data on a popular hacking forum. The data was for sale for US$500,000.

USD 257 million seized in global police crackdown against online scams

A global police operation spanning 61 countries has delivered a financial blow to online scam networks by freezing 6,745 bank accounts, seizing assets totalling USD 257 million, and disrupting the transnational organized crime networks involved. Targeting phishing, investment fraud, fake online shopping sites, romance and impersonation scams, Operation First Light 2024 led to the arrest of 3,950 suspects and identified 14,643 other possible suspects in all continents. Police collectively intercepted some USD 135 million in fiat currency and USD 2 million in cryptocurrency. Fiat currency, such as the US Dollar, Euro, or Yen, is official currency issued and regulated by governments. Other assets worth over USD 120 million were seized, including real estate, high-end vehicles, expensive jewellery, and many other high-value items and collections.

Summary of last month’s Cyber Alerts and News Clips:

Incident Response Solutions post certain alerts and tips we consider to be in the public interest as it comes to hand. We publish these alerts and tips on this webpage.

12/06/2024 – NCSC – Phishing campaign targeting New Zealand organisations

Our Views:

New Centre for Internet Security (CIS) Version 8.1

CIS has just released an iterative update to the CIS security controls version 8.0. The CIS Controls version 8.1 is guided by the design principles of context, clarity, and consistency. The CIS Controls aim to simplify the design, implementation, measurement, and management of enterprise security which involves:

- Simplifying language to reduce duplication.
- Focusing on measurable actions with defined metrics.
- Ensuring each safeguard is clear and concise.

What has changed?

Specific Updates in CIS Controls v8.1 include:

- Realigned NIST CSF Security Function Mappings: Adjustments have been made to match NIST CSF 2.0.
- Expanded Glossary Definitions: New and expanded definitions for terms such as "plan," "process," and "sensitive data" have been included.
- Revised Asset Classes and Mappings: Asset classes have been revised, and new mappings to safeguards have been introduced.
- Typographical Corrections: Minor typos in safeguard descriptions have been fixed.
- Clarified Safeguard Descriptions: Clarifications have been added to several safeguard descriptions to ensure they are clear and actionable.

We have reviewed the specific changes to the safeguard descriptions in IG1 and outline below what you need to know about these.

For each of the IG1 controls listed below the safeguard descriptions have each been updated to prescribe and emphasise the need for “documented” processes. CIS 8.0 safeguard descriptions highlighted the need for a process in each area however CIS 8.1 clarifies that each of these should be a “documented” process.

- CIS 2.1 Establish and Maintain a Software Inventory
- CIS 3.1 Establish and Maintain a Data Management Process
- CIS 4.1 Establish and Maintain a Secure Configuration Process
- CIS 5.1 Establish and Maintain an Inventory of Accounts
- CIS 6.1 Establish and Access Granting Process
- CIS 8.1 Establish and Maintain an Audit Log Management Process
- CIS 11.1 Establish and Maintain a Data Recovery Process

For some safeguards CIS 8.1 clarifies scope or adds additional detail to the safeguard as follows:

- CIS 12.2 Establish and Maintain a Secure Network Architecture (Adds a requirement for policy and design components to be reflected in the implementation)
- CIS 14.2 Train workforce members to recognise social engineering attacks (Adds a specific requirement for Business Email Compromise training).

An additional addition to v8.1 is the inclusion of the “Governance” security function. Effective governance is crucial for steering a cybersecurity program towards achieving enterprise goals. The Controls now specifically identify governance topics as recommendations, helping users implement these to enhance their cybersecurity governance.

A full log of all changes made in this version is available here.

Next Steps

The CIS controls strive to balance addressing current cybersecurity challenges while maintaining a stable foundational cyber defence strategy. Rapid developments in technology, including artificial intelligence, augmented reality, and ambient computing, are constantly under review and CIS note that they are already working on ideas for version 9 of the CIS Controls to stay ahead of these advancements.

However, this latest update ensures minimal disruption for existing users by not modifying any Implementation Groups and maintaining the core intent of each safeguard. As such, we believe it is perfectly reasonable to remain scoring on the CIS version 8.0 if this is your current practice and update to CIS v8.1 when next practical.

About the Bulletin:

The NZ Incident Response Bulletin is a monthly high-level executive summary containing some of the most important news articles that have been published on Forensic and Cyber Security matters during the last month. Also included are articles written by Incident Response Solutions, covering topical matters. Each article contains a brief summary and if possible, includes a linked reference on the web for detailed information. The purpose of this resource is to assist Executives in keeping up to date from a high-level perspective with a sample of the latest Forensic and Cyber Security news.

To subscribe or to submit a contribution for an upcoming Bulletin, please either visit https://incidentresponse.co.nz/bulletin or send an email to bulletin@incidentresponse.co.nz with the subject line either "Subscribe", "Unsubscribe", or if you think there is something worth reporting, "Contribution", along with the Webpage or URL in the contents. Access our Privacy Policy.

Subscribers to the premium edition also obtain access to the following additional information:

- Cyber Governance
- Cyber Incident Landscape
- Cyber Incident Response Resources
- Cyber Framework and Control Updates, Surveys and Research

Click here if you wish to subscribe to our Premium Edition of the Bulletin.

About Incident Response Solutions Limited:

Our Purpose - We help you with specialist forensic, cyber security and crisis management expertise at all stages throughout the incident response lifecycle.

Our Promise - We will provide you with the confidence you require to prepare, respond and recover from forensic and cyber incidents.

Our specialist Forensic Technology expertise includes Computer Forensics, Cybercrime Incident Response, Social Media Analysis and eDiscovery. We have significant experience in providing expert witness reports and in delivering expert witness testimony at trial. Our background includes experience in Law Enforcement (NZ Police) and Big 4 Professional Services.

Campbell McKenzie
Director
Incident Response Solutions Limited
0800 WITNESS
+64 21 779 310
campbell@incidentresponse.co.nz

This Bulletin is prepared for general guidance and does not constitute formal advice. This information should not be relied on without obtaining specific formal advice. We do not make any representation as to the accuracy or completeness of the information contained within this Bulletin. Incident Response Solutions Limited does not accept any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, when relying on the information contained in this Bulletin or for any decision based on it.

Further Resources:

Alerts	Data Breach Response	Forensic Technology
Cyber Incident Simulations	Social Media Investigations	Guide for NZ Law Firms

Share our Bulletin: