NCSC

National Cyber Security Centre

2407190120-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

CrowdStrike BSOD Loop Issue

UPDATE - Version 1.1

Friday 19th July, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.*

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/.

Please treat this document in accordance with the TLP assigned.

Revision History

Revision	Date	Author(s)	Description
1.0	19th July 2024	CSIRT-IE	Initial advisory
1.1	19th July 2024	CSIRT-IE	Update with further steps

Description

The NCSC is aware of an issue with falcon agent which may cause issues when booting machines. Symptoms include hosts experiencing a bugcheck or bluescreen error related to Falcon Sensor. CrowdStrike are actively working on a fix and there is no need to contact support; a public statement by CrowdStrike can be found at the following link: https://www.crowdstrike.com/blog/statement-on-windows-sensor-update/. Further information:

- Windows hosts which have not been impacted do not require any action as the problematic channel file has been reverted.
- Windows hosts which are brought online after 0527 UTC will also not be impacted
- Hosts running Windows7/2008 R2 are not 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.

Current Action

CrowdStrike have identified a content deployment related to this issue and reverted those changes. If hosts are still crashing and unable to stay online to receive the Channel File Changes, the following steps can be used to workaround this issue.

Workaround Steps

Workaround Steps for individual hosts:

- Boot Windows into Safe Mode or the Windows Recovery Environment
  - Putting the host on a wired network (as opposed to WiFi) and using Safe Mode with Networking can help remediation.
- Navigate to

```
C:\Windows\System32\drivers\CrowdStrike
```

- Locate the file matching “**C-00000291*.sys**”, and delete it.
- Boot the host normally.
  - **Note:** Bitlocker-encrypted hosts may require a recovery key.

Workaround Steps for public cloud or similar environment including virtual:

- Option 1
  - Detach the operating system disk volume from the impacted virtual server
  - Create a snapshot or backup of the disk volume before proceeding further as a precaution against unintended changes
  - Attach/mount the volume to to a new virtual server
  - Navigate to

`C:\Windows\System32\drivers\CrowdStrike`

  - Locate the file matching "**C-00000291*.sys**", and delete it.
  - Detach the volume from the new virtual server
  - Reattach the fixed volume to the impacted virtual server

- Option 2
  - Roll back to a snapshot before 0409 UTC.

AWS-specific documentation:

- To attach an EBS volume to an instance: https://docs.aws.amazon.com/ebs/latest/userguide/ebs-attaching-volume.html#:~:text=To%20attach%20an%20EBS%20volume,and%20choose%20Actions%2C%20Attach%20volume
- Detach an Amazon EBS volume from an instance: https://docs.aws.amazon.com/ebs/latest/userguide/ebs-detaching-volume.html

Azure environments:

- Please review https://azure.status.microsoft/en-gb/status

Bitlocker recovery-related KBs:

- BitLocker recovery in Microsoft Azure: https://www.crowdstrike.com/wp-content/uploads/2024/07/BitLocker-recovery-in-Microsoft-Azure.pdf
- BitLocker recovery in Microsoft environments using SCCM: https://www.crowdstrike.com/wp-content/uploads/2024/07/BitLocker-recovery-in-Microsoft-environments-using-SCCM.pdf
- BitLocker recovery in Microsoft environments using Active Directory and GPOs: https://www.crowdstrike.com/wp-content/uploads/2024/07/BitLocker-recovery-in-Microsoft-environments-using-Active-Directory-and-GPOs.pdf
- BitLocker recovery in Microsoft environments using Ivanti Endpoint Manager: https://www.crowdstrike.com/wp-content/uploads/2024/07/BitLocker-recovery-in-Microsoft-environments-using-Ivanti-Endpoint-Manager.pdf

General Awareness

Increased Phishing Attempts During IT Outages

Please be aware of opportunistic phishing attempts culminating from this Global IT outage event. Be extra cautious of emails, calls or texts claiming to be from IT support. Always verify the sender's details and never click on links or open attachments provided through unexpected channels.

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
Tom Johnson House,
Beggars Bush,
Dublin, D04 A068,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie

An Lárionad Náisiúnta
Cibearshlándála
National Cyber Security Centre