SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | **IT-ASSETS**

Fehlerhaftes Update von Crowdstrike Falcon

CSW-Nr. 2024-257485-10F1, Version 1.0, 19.07.2024

IT-Bedrohungslage*: 3 / Orange

Sachverhalt

Crowdstrike Falcon ist eine weit verbreitete Enterprise Detection und Response (EDR) Schutzsoftware für Endgeräte. Während des Betriebs werden regelmäßig Softwareupdates mittels sogenannter Channel-Dateien ausgerollt. Mit Hilfe der Channel-Dateien verteilt Crowdstrike dynamische Updates und Detektionsregeln.

Durch ein jüngst ausgerolltes fehlerhaftes Update, welches die auf Endgeräten und Servern installierten Crowdstrike Falcon Sensoren betrifft, kam es zu einer Situation, die unter Windows zu Abstürzen führen kann.

Laut dem Hersteller Crowdstrike sind Systeme betroffen, die eine Channel-Datei "C-00000291*.sys" mit einem Zeitstempel von 04:09 UTC 19.07.2024 installiert haben. Sollte die Datei einen Zeitstempel von 05:27 UTC oder von einem späteren Zeitpunkt aufweisen, handelt es sich um eine fehlerbereinigte Version, die nicht betroffen ist.

Systeme, die über Nacht ausgeschaltet waren und erst nach 05:27 UTC eingeschaltet wurden, sind nach Aussage des Herstellers nicht betroffen [CRO 1]. Des Weiteren sind auch keine Linux oder MacOS Systeme mit einem Falcon Sensor betroffen.

Microsoft berichtet hingegen, dass sie bereits um 19:00 UTC 18.07.2024 erste Ausfälle beobachtet haben [MSO 1].

Aufgrund der weltweiten Verbreitung des Tools kommt es zu großflächigen Störungen bei einer Vielzahl von Organisationen.

Mehrere Betreiber von Kritischer Infrastrukturen aus verschiedenen Sektoren meldeten dem BSI gem. § 8b Abs. 4 BSIG Betroffenheiten sowie teils Einschränkungen in der Erbringung der kritischen Dienstleistung.

Bewertung

Die Störung hat vereinzelt zu teils gravierenden Einschränkungen im Geschäftsbetrieb von verschiedenen Unternehmen geführt.

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb: IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange: Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Bisher liegen keine Informationen bezüglich einer Betroffenheit von Privatanwendern vor. Da es sich um ein Enterprise Tool handelt, geht das BSI nicht von einer Betroffenheit bei Privatanwendern aus.

Hinweis für Betreiber Kritischer Infrastrukturen: Sollte eine Betroffenheit von der hier beschriebenen Störung bestehen, so kann die Meldung nach § 8b Abs. 4 BSIG über die etablierten Meldewege abgegeben werden. Sollte der zu meldende Sachverhalt nicht über den dieser Management-Information hinausgehen, so ist ein Verweis auf die vorliegende Management-Information als inhaltliche Beschreibung ausreichend. Bitte führen Sie jedoch in jedem Fall die Auswirkungen auf Ihren Betrieb im Falle einer Meldung aus.

Aktuell ist noch keine Bewertung hinsichtlich des genauen Beginns der Ausfälle durch die fehlerhafte Datei möglich, da die Aussagen des Herstellers und von Microsoft diesbezüglich divergieren.

Der Sachverhalt kann exemplarisch für die Schäden angesehen werden, die eintreten können, wenn die Anforderungen des Bausteins OPS.1.1.3 Patch- und Änderungsmanagement aus dem IT-Grundschutz Kompendium nicht umgesetzt werden.

Maßnahmen

Der Hersteller nennt in seinem Tech Alert [CRO 1] mehrere Workarounds, die nachfolgend wörtlich zitiert werden:

Individuelle Systeme

- Reboot the host to give it an opportunity to download the reverted channel file. If the host crashes again, then:
- Boot Windows into Safe Mode or the Windows Recovery Environment
- Navigate to the C:\Windows\System32\drivers\CrowdStrike directory
- Locate the file matching “C-00000291*.sys”, and delete it.
- Boot the host normally.
- Note: Bitlocker-encrypted hosts may require a recovery key

Cloudsysteme und virtualisierte Systeme

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 the C:\Windows\System32\drivers\CrowdStrike directory
- 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 04:09 UTC

Microsoft Azure Systeme

Workaround Steps for Azure via serial

1. Login to Azure console --> Go to Virtual Machines --> Select the VM

2. Upper left on console --> Click : "Connect" --> Click --> Connect --> Click "More ways to Connect" --> Click : "Serial Console"
3. Step 3 : Once SAC has loaded, type in 'cmd' and press enter.
    1. type in 'cmd' command
    2. type in : ch -si 1
4. Press any key (space bar). Enter Administrator credentials
5. Type the following:
    1. bcdedit /set {current} safeboot minimal
    2. bcdedit /set {current} safeboot network
6. Restart VM
7. Optional: How to confirm the boot state? Run command:
    - wmic COMPUTERSYSTEM GET BootupState

Weitergehende Informationen sollen sich auf [MSO 1] finden.

Weitere Hinweise

Bei mit Bitlocker verschlüsselten Systemen sollte vor einem Neustart Bitlocker deaktiviert werden und sichergestellt werden, dass der Recovery Key gesichert und offline zugänglich ist.

Es gibt vereinzelte Berichte, dass es ggf. ausreicht in den "Windows Safe Mode with Network" zu booten und abzuwarten, bis die fehlerhafte Datei automatisch durch ein Update ersetzt wird. Grundsätzlich sollte sich an die oben genannten Workaround-Hinweise des Herstellers gehalten werden.

Links

[CRO 1], Tech Alert | Windows crashes related to Falcon Sensor | 2024-07-19 (Abruf nur mit Account möglich), https://supportportal.crowdstrike.com/s/article/Tech-Alert-Windows-crashes-related-to-Falcon-Sensor-2024-07-19
[MSO 1] , Azure Status, https://azure.status.microsoft/en-gb/status