TLP: GREEN

Summary:
CrowdStrike is aware of reports of crashes on Windows hosts that have taken place after installing the latest update for CrowdStrike Falcon Sensor. CrowdStrike says that it has identified a content deployment related to this issue and reverted those changes.

Impact:
The issue has not impacted Linux and Mac hosts. Windows hosts are being stuck in a boot loop or experiencing bugcheck/blue screen errors related to the Falcon Sensor.
Note: Hosts running Windows 7/2008 R2 are not impacted.

Several organizations and services across the world have been impacted, including airports, airlines, banks, hospitals, as well as emergency services such as 911. There have been growing concerns over supply chain security, with airlines like Delta and United Airlines stating that third-party outages have impacted computer systems worldwide, further causing delays in flight departures. Microsoft Azure also reported issues with Virtual Machines running Windows Client and Windows Server with the CrowdStrike Falcon agent, encountering a bug check (BSOD) and getting stuck in a restarting state. While the impact has been widespread, systems are gradually being brought back online. Customers still experiencing issues should contact CrowdStrike for support.

Mitigation:
The root cause has been associated with a Channel File, which contains data for the Falcon Sensor. CrowdStrike has reverted the Channel file. Note: 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. Hosts booted up after 5:27 AM UTC should not be experiencing any issues. If hosts are still crashing and unable to stay online to receive the Channel File Changes, CrowdStrike recommends:

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

Sources:
- https://www.crowdstrike.com/blog/statement-on-windows-sensor-update/
- https://x.com/George_Kurtz/status/1814235001745027317
- https://www.cnet.com/tech/services-and-software/microsoft-global-outage-explained-911-lines-down-flights-grounded-and-more/