Major Incident Report: CrowdStrike Falcon Sensor Outage (July 2024)

Prepared by: IT Operations

Prepared for: Executive & Retail Leadership

Document version: 1.0

Executive Summary

On July 19, 2024, a faulty CrowdStrike Falcon **Windows** sensor content update (“Channel File 291”) propagated globally and caused Blue Screen of Death (BSOD) crashes on millions of Windows endpoints. The defective update was rolled back by CrowdStrike within ~78 minutes of release, but many devices required manual remediation before returning to service. This document summarizes the impact, timeline, root cause, response, and preventive actions for our organization.

Impact (Organization)

Business units affected	**Retail stores, POS registers, kiosks, back■office Windows workstations, som**
Geography	Multi■state (U.S.), including Central time (CDT) sites
Primary symptoms	BSOD loop, error codes 0x50 / 0x7E; systems auto■restarting; Falcon agent bugch
Duration (customer■visible)	Peak disruption on July 19 (CDT morning) with recovery activities through the week
Customer impact	Checkout delays, temporary loss of workstation access, manual payment fallbacks
Security impact	No evidence of malicious activity; incident stemmed from vendor update defect

Timeline (Key Events)

2024■07■18 23:09 CDT (2024■07■19 04:09 UTC)	**CrowdStrike releases Windows Falcon sensor content update (Channe**
2024■07■19 00:27 CDT (05:27 UTC)	CrowdStrike rolls back the problematic content update.
2024■07■19 02:00–08:00 CDT	Wide BSOD reports across industries; our retail sites report register and ba
2024■07■19 08:30 CDT onward	Begin staged remediation per vendor guidance; bring priority endpoints (PC
2024■07■20 to 2024■07■21	Clean■up of offline/remote devices and kiosk endpoints; confirm Falcon he

Root Cause

The vendor confirmed a logic error in the Falcon Windows sensor content configuration that led to an out■of■bounds memory read in the Windows kernel and subsequent bugchecks (BSOD). The issue was not malicious and did not affect macOS or Linux sensors.

Detection & Triage

Detection was external and near■simultaneous via vendor advisories, national CERT/CISA alerts, and a spike in internal monitoring/ticket volume from stores and kiosks. Our triage confirmed impact correlated to endpoints running the CrowdStrike Falcon Windows agent.

Response Summary (Our Org)

1) Declared a Major Incident; established a war■room bridge and retail leadership comms.

2) Prioritized POS registers and critical back■office systems.

3) Applied vendor remediation: boot to Safe Mode or Recovery, isolate from network if needed, remove the bad content file, update/repair Falcon sensor, and reboot to normal mode.

4) Staggered bring■up and validation (payment, printing, network join, EDR health).

5) Post■incident sweep for stragglers and policy drift.

Remediation Procedures (High■Level)

A) For affected Windows endpoints in BSOD loop:

• Attempt multiple restarts; if still failing, boot to Safe Mode/WinRE.

• Remove or replace the problematic Falcon channel file per vendor KB, ensure sensor is updated to a fixed content version.

• Reboot, confirm stability, verify Falcon sensor and Windows Defender/Firewall status.

B) For unaffected devices coming online after rollback:

• No action required beyond standard health checks.

C) Servers and kiosks:

• Use maintenance windows; validate line■of■business apps and peripherals (printers, PIN pads).

Communications

• Internal: hourly updates to execs/retail ops during peak; store■facing bulletin with simple steps and escalation contacts. • External: monitored vendor advisories; mirrored guidance in our KB; notified third■party partners where access was affected.

Preventive & Hardening Actions

• Adopt staggered/phased EDR content rollout rings with rapid canary feedback before global release.

• Strengthen offline/remote remediation playbooks (USB/WinRE media, Safe Mode SOPs).

• Ensure site failover procedures and manual payment fallbacks are documented and tested.

• Enhance device compliance checks (EDR health, reboot debt) and ensure kiosk/remote assets are manageable.

• Vendor management: require RCA, SLAs for rollback gates, and emergency comms channels.

References

Primary sources (for audit): – CrowdStrike Technical Details (07/20/2024) and Channel File 291 RCA (08/06/2024). – CrowdStrike Tech Alert PDF (07/19/2024). – Microsoft KB5042421 guidance (Windows BSOD 0x50/0x7E). – CISA/CIS advisory notes and public timeline corroboration.

Appendix A: Quick Recovery Checklist

Step	Action
1	If in BSOD loop, try 2–3 restarts; if unresolved, boot to Safe Mode/WinRE.
2	Disconnect from network if needed; apply vendor guidance to remove/replace faulty channel file.
3	Update/repair Falcon sensor; reboot; verify login and stability.
4	Validate POS peripherals (printers, PIN pad), network join, and line■of■business apps.
5	Confirm Falcon health, Windows Update, and backup/restore points.