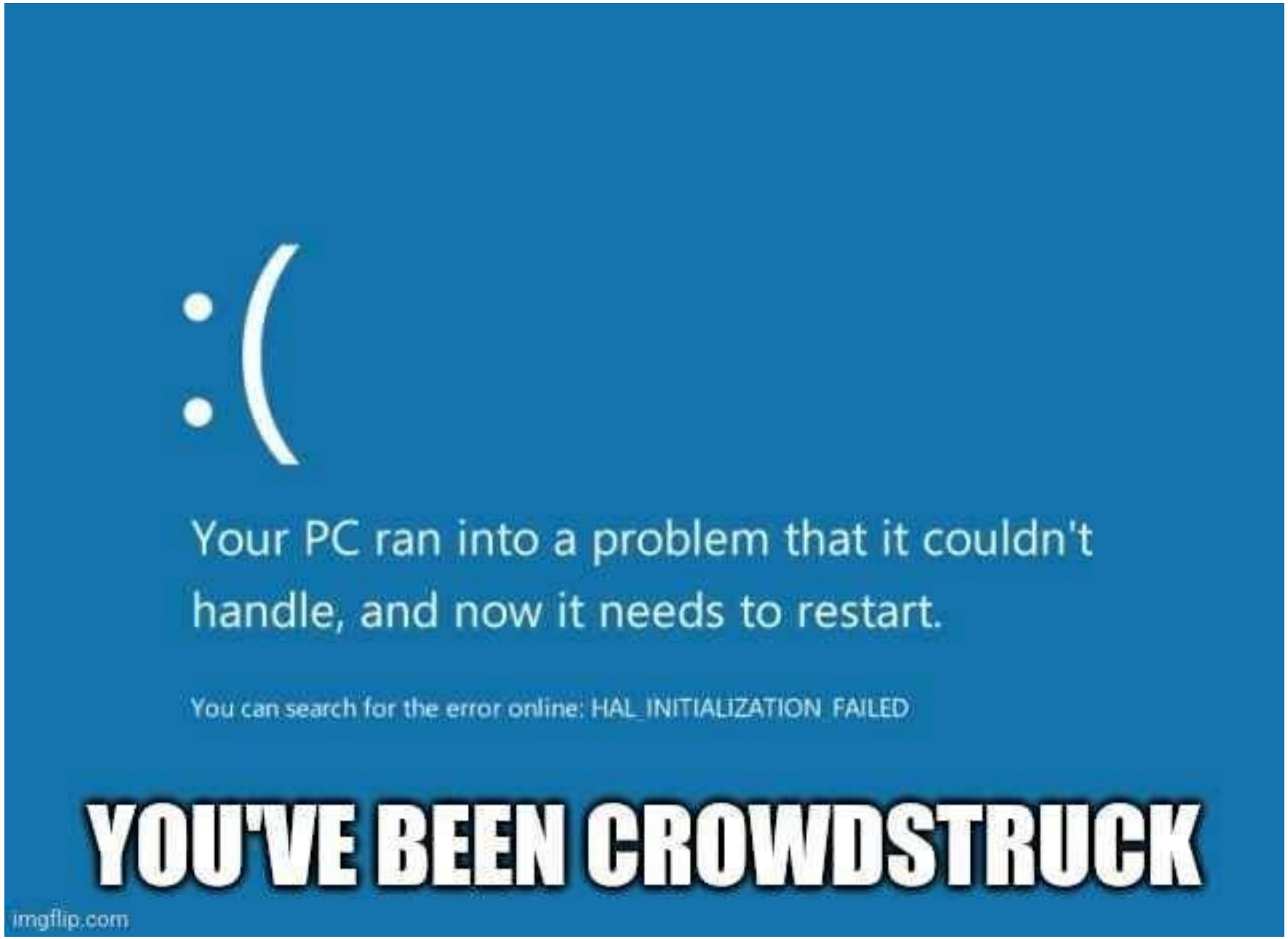
Indian Health Service
CrowdStrike Update

REESE WEBER, MBA, CISSP

2024 BEST PRACTICES CONFERENCE

MAY 20-22, 2024


:(
Your PC ran into a problem that it couldn't handle, and now it needs to restart.
You can search for the error online: HAL_INITIALIZATION_FAILED
YOU'VE BEEN CROWDSTRUCK
imgflip.com

What is CrowdStrike?

CrowdStrike is a cybersecurity company that offers cloud-based software and services to protect businesses from cyber threats.

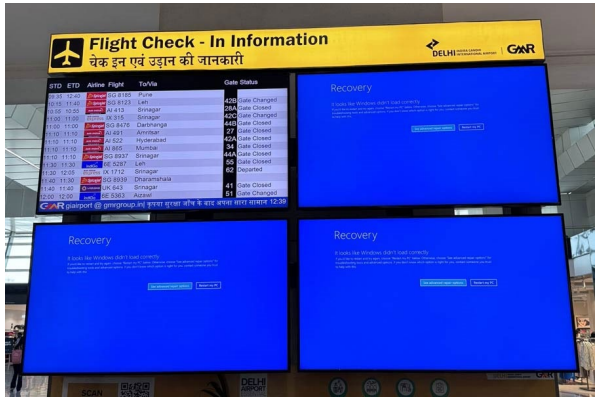
Their Falcon platform, a cloud-based solution that combines multiple security solutions into a single hub, including antivirus capabilities, endpoint protection, threat detection, and real-time monitoring to prevent unauthorized access to a company's system.

Their software is utilized by over 50% of the Fortune 1000 Companies, many government bodies and the nation's top cybersecurity agency, Cybersecurity and Infrastructure Security Agency.

What Happened?

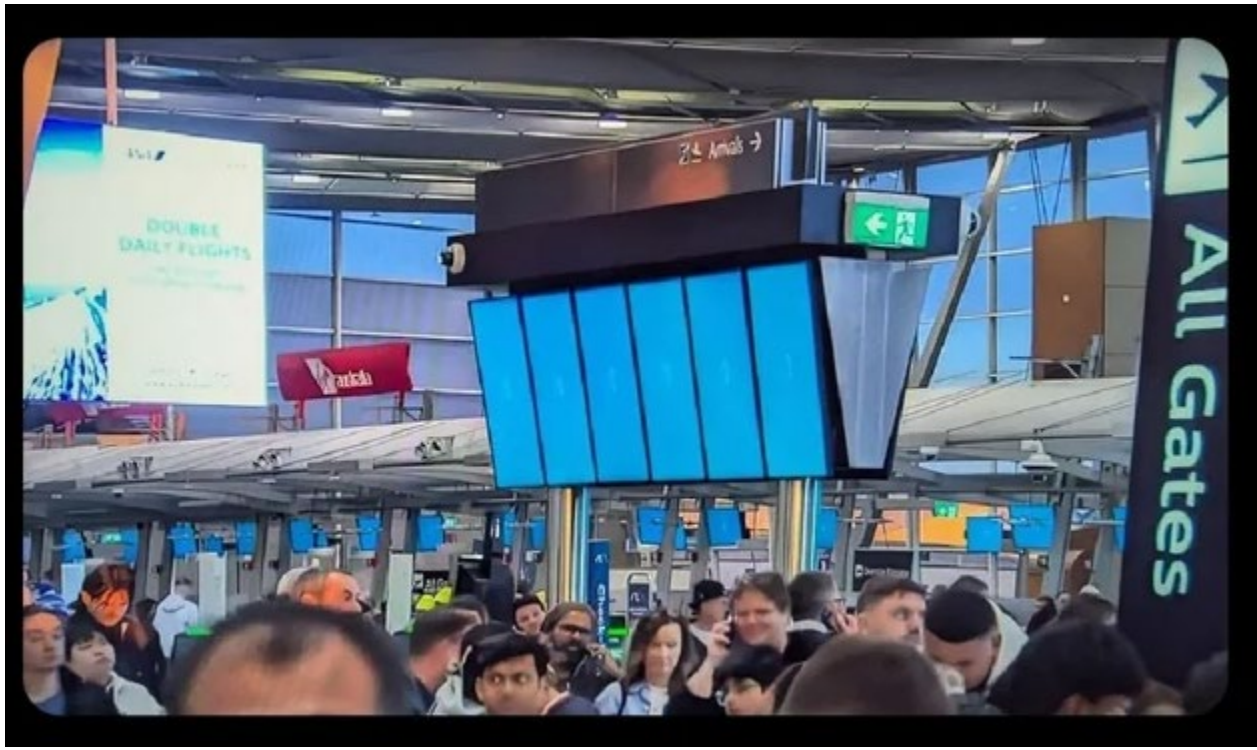
- July 18, 2024, 9 PM PST, CrowdStrike pushed a faulty sensor configuration update to the millions of PCs worldwide running its Falcon Sensor software.
- Sensors expected 20 input fields, while the update provided 21 input fields. In this instance, the mismatch resulted in an out-of-bounds memory read, causing a system crash.
- Microsoft estimates that this event affected 8.5 million Windows devices.
- Affected Systems displayed blue screens and most had to be manually recovered because the systems needed to boot into Safe Mode to mitigate.

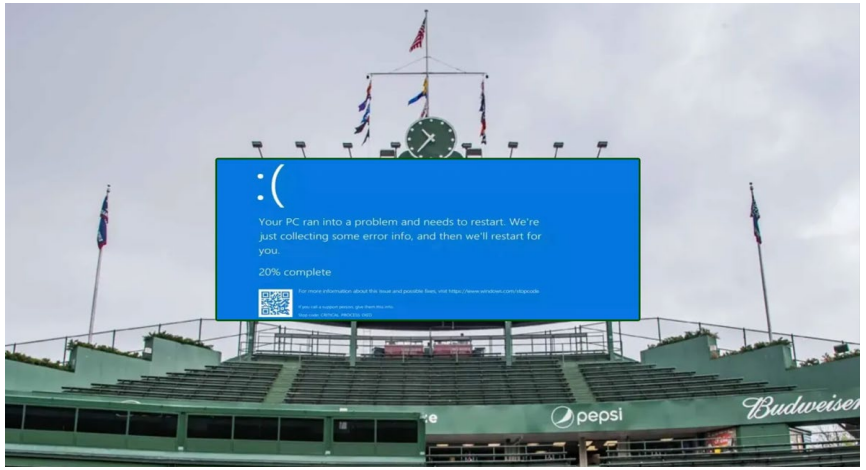
Times Square, New York City



Dehli Airport, India

Sydney Airport, Australia





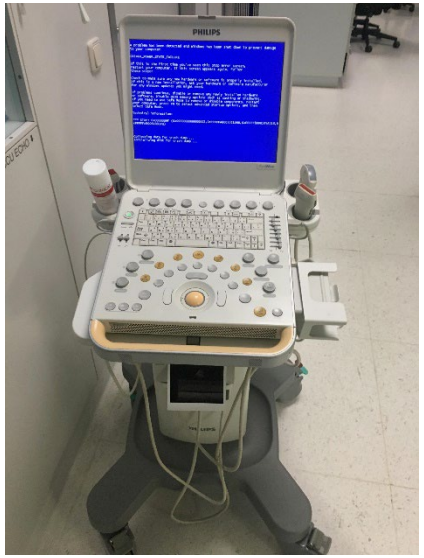
Wrigley Field, Chicago

Impact on IHS Systems

35 Domain Controllers affected

8,000+ of 23,000 IHS endpoints affected (35% of IHS systems)

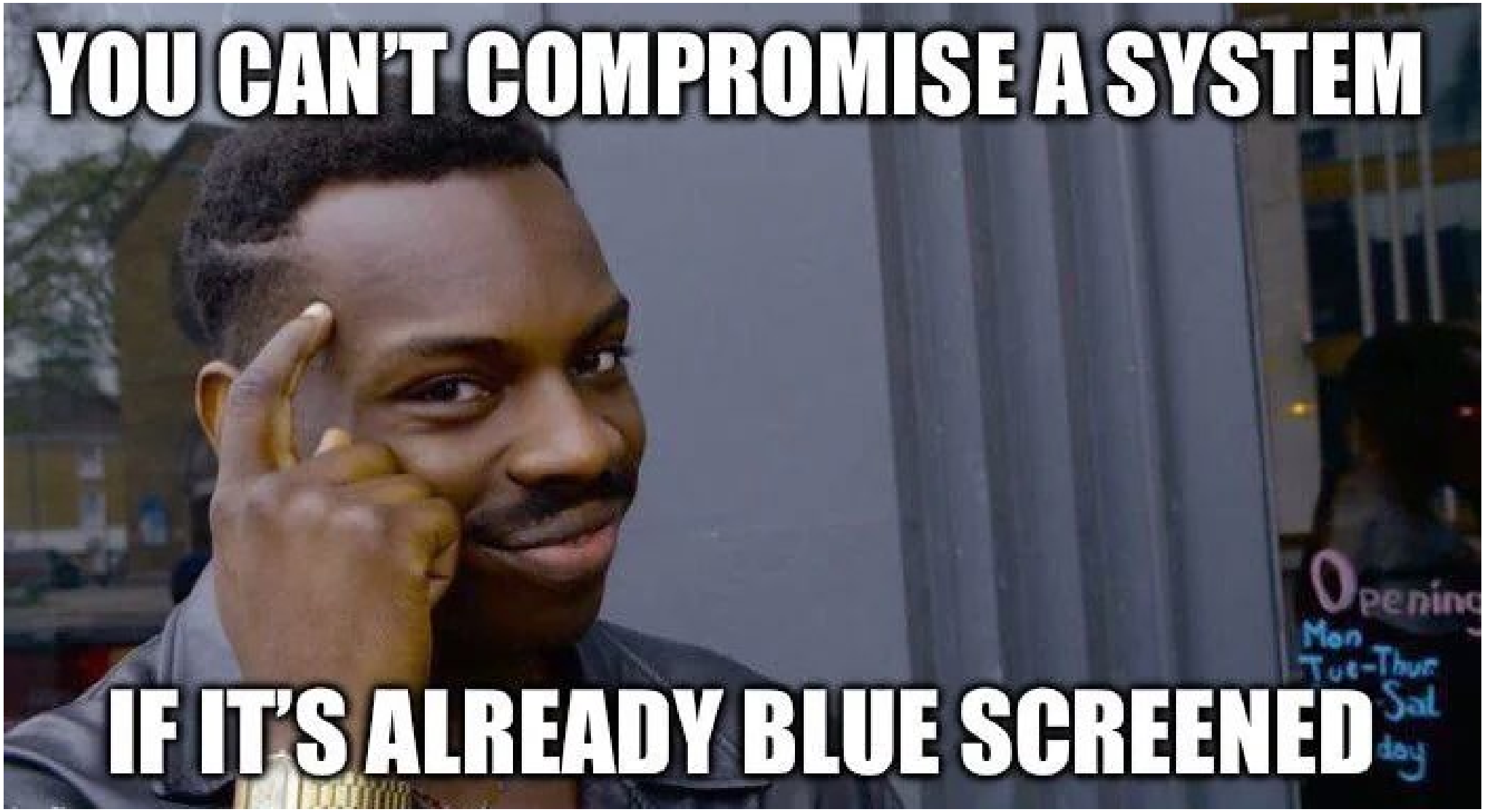
- 3,000 + endpoints resolved within 4.5 hours
- By Monday (1 Business Day), there were about 2,000 systems still affected (9%)
- By Friday (5 Business Days) there was about 700 systems left (3.2%)
- Currently (21 Business Days) we have >200 systems left (.8%)



Impact on California Area Systems

Clinical impact for Tribal/Urban Programs Using RPMS

- Practice Management Application Suite (BPRM) affected:
  - Area hosted RPMS Database health programs were temporarily unable to schedule appointments using the Graphical User Interface (GUI). RPMS roll and scroll was recommended as an alternative method for scheduling. Services restored at 12:50 pm
- California Immunization Registry (CAIR) affected:
  - Area hosted RPMS Database health programs were temporarily unable to access the California Immunization Registry Services restored at 1:40 pm
- IHS California Area Print Server affected:
  - About half of our Area hosted RPMS Database health programs were temporarily unable to print from RPMS Services restored at 2:20 pm
- IHS California Area Terminal Server affected:
  - Contractors providing Lab, Prescribing and Clinical Access Coordination were temporarily unable to log into our terminal server to provide support to sites. Services restored at 2:40 pm


YOU CAN'T COMPROMISE A SYSTEM
IF IT'S ALREADY BLUE SCREENED

Questions?

Reese Weber, MBA, CISSP

Chief Information Security Officer and Privacy Coordinator

Indian Health Service, California Area

916-930-3981 x 307

Theresa.weber@ihs.gov

https://www.linkedin.com/in/reese-weber-mba-cissp-6085203b

References:

https://www.theverge.com/2024/7/19/24201864/crowdstrike-outage-explained-microsoft-windows-bsod

https://www.zdnet.com/article/what-caused-the-great-crowdstrike-windows-meltdown-of-2024-history-has-the-answer/

https://fedscoop.com/federal-government-agencies-affected-by-worldwide-it-outage/

https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/


INDIAN HEALTH SERVICE
PHS
1955