Cal OES
GOVERNOR'S OFFICE OF EMERGENCY SERVICES

CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

TLP:CLEAR
19 July 2024

CrowdStrike Falcon Sensor Defect

Crowdstrike | Falcon Sensor | Blue Screen | Windows

The California Cybersecurity Integration Center (Cal-CSIC) is monitoring an ongoing issue where users/customers were impacted by a defect found in a single content update for Windows hosts related to the Crowdstrike Falcon Sensor.[1] This defect causes hosts to experience bug check and bluescreen errors, causing affected Windows systems to stop running.

Despite the effects of this content update, Crowdstrike posted that this is not a cyber-attack or cyber incident.[1] The Cal-CSIC assesses that based on current and available reporting there is no evidence to support the contrary.

This defect has already caused some grounded flights, knocked some banks offline, and massive disruption impacting companies and services around the world.[3]

There are several workarounds depending on the specifics of the impacted operating system. Cal-CSIC recommends following the workaround steps posted by Crowdstrike.[1] For further information please refer to Statement on Falcon Content Update for Windows Hosts - crowdstrike.com

During this time, the Cal-CSIC recommends increased vigilance in cyber security awareness for all users. This is a prime opportunity for bad actors to pose as Crowdstrike and take advantage of the disruption including through phishing attempts. Cal-CSIC analysts have been alerted to a number of domains that have been registered or reported as phishing domains in the past 24 hours likely related to this outage. Please exercise caution when using search engines and clicking on links related to Crowdstrike and the current outage. Some examples of recently registered domains include:

crowdstrike-bsod[.]com
crowdstrikebluescreen[.]com
microsoftcrowdstrike[.]com
fix-crowdstrike-bsod[.]com
fix-crowdstrike-apocalypse[.]com
crowdstrike0day[.]com

For any support requests please reach out to calcsic_watch@caloes.ca.gov or call 833-737-6781.

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] CrowdStrike; "Statement on Falcon Content Update for Windows Hosts;" https://www.crowdstrike.com/blog/statement-on-falcon-content-update-for-windows-hosts/; accessed 19 July 2024

[2] Bleeping Computer "CrowdStrike update crashes Windows systems, causes outages worldwide" https://www.bleepingcomputer.com/news/security/crowdstrike-update-crashes-windows-systems-causes-outages-worldwide/; accessed 19 July 2024

[3] APNews "Global tech outage live updates: Flights grounded and offices hit as internet users face disruptions" https://apnews.com/live/internet-global-outage-crowdstrike-microsoft-downtime#; accessed 19 July 2024

CAL-CSIC-202406-007

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

TLP:CLEAR

2