



KPMG Cyber Threat Intelligence Platform

CrowdStrike Causing Global Windows Outage



CrowdStrike, a leading cybersecurity platform providing advanced solutions worldwide, is currently experiencing a significant outage affecting users globally. The issue primarily manifests as Blue Screen of Death (BSOD) errors on Windows systems due to a technical error in their main product, Falcon Sensor. The issue, which seemingly affects multiple versions of Windows has been observed following the latest updates of the CrowdStrike agent. This outage has numerous individual users and organizations across countries such as Croatia, Philippines, US, Germany, Mexico, India, and Japan.

CrowdStrike has acknowledged reports of widespread crashes on Windows systems attributed to the Falcon Sensor. Symptoms include hosts experiencing bugchecks and BSOD errors specifically related to 'csagent.sys'. This issue has resulted in extensive disruption, with reports indicating over 3,000 laptops and servers affected across multiple locations in Australia and New Zealand alone, and similar impacts reported globally. Affected users, including defense agencies, banks, payroll services, major retailers, and individual consumers, have been advised by CrowdStrike to refrain from opening support tickets at this time, while the engineering teams are actively working to resolve the issue. While the company is focusing on fixing the underlying problem causing the BSOD errors, concerns regarding the restoration of devices currently stuck in boot loops even after the issue is resolved still remain.

In response CrowdStrike has provided a workaround for users experiencing persistent crashes on their Windows systems due to ongoing issues. If hosts cannot stay online to receive Channel File Changes, users should follow these steps:

- Boot into Safe Mode or Windows Recovery Environment.
- Navigate to C:\Windows\System32\drivers\CrowdStrike.
- Delete the file matching "C-00000291*.sys" or rename it to "C-00000291*.sys.renamed" and reboot the host normally.

File integrity verification may cause issues with this workaround and shall be disabled before performing the above steps. Further, it must be noted that this workaround may not work on LAPS or Bitlocker enabled systems and further fix is awaited.

The KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/TAXII/MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:

Strategic threat intelligence report

Machine ingestible threat intelligence feeds

Threat intelligence driven pre-emptive threat hunting exercise

Cyber Incident Response Services

Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471

Atul Gupta
Partner, Head of Cyber Security,
KPMG in India
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner, KPMG in India
T: +91 98455 45202
E: raghavendrabbv@kpmg.com

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Partner,
KPMG in India
T: +91 98181 99432
E: mtembhurkar@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2024 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

#KPMGjoshi

home.kpmg/in

Follow us on home.kpmg/in/socialmedia





KPMG Cyber Threat Intelligence Platform

CrowdStrike Causing Global Windows Outage



Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

20% complete



For more information about this issue and possible fixes, visit <https://www.windows.com/stopcode>

If you call a support person, give them this info:
Stop code: CRITICAL_PROCESS_DIED

Recovery

It looks like Windows didn't load correctly

If you'd like to restart and try again, choose "Restart my PC" below. Otherwise, choose "See advanced repair options" for troubleshooting, tools and advanced options. If you don't know which option is right for you, contact someone you trust to help with this.

See advanced repair options

Restart my PC