█████████-Crowdstrike Outage

██████████████████████████████

█████████

* ██████████████
* Global Impact
* Technical Background
* Assessment
* Annexure

Report on global IT outage █████████ – CrowdStrike of 19th July 2024:

Brief Summary

On 19th July 2024, a massive IT outage affected businesses and critical services globally, with ███████████████ and █████████████ services experiencing widespread disruptions.

The issue started on 19 July 2024 at 04:09 ███ (09:39 hours ███) and is currently in various stages of recovery. Users experienced ████████████████████████ (BSOD) error, which caused their systems to shut down or restart unexpectedly.

The root cause was found to be a faulty content update from cyber security provider ███████████ of its falcon server, affecting countless windows PCs and services across various sectors. According to ███████, an established market research firm, ███████████ accounts for 14 percent of the security software market by revenue, meaning its software is on a wide array of systems.

Technical workarounds have been prescribed and a fix has been deployed. As per various sources including both █████████, ███████████ and partner country agencies, this is not a result of a cyber-attack.

Global Impact

Globally, over 42,000 flights delayed on 19th July 2024. In the US, Delta, ██████, and █████████████████ grounded all flights at least temporarily.

In the UK, Israel, and Germany, health care services and hospitals saw systems that they use to communicate with patients disrupted, and cancelled some appointments.

Emergency services in the US using 911 have reportedly had problems with their lines too. In the earliest hours of the outages, some TV stations, including ████████ in the UK, stopped live news broadcasts.

Technical Background

█████████ confirmed that the issue started on 19 July 2024 at 04:09 ███ (09:39 hours ███), which resulted in customers experiencing unresponsiveness and startup failures on Windows machines using the CrowdStrike Falcon agent, affecting both on-premises and various cloud platforms (Azure, ███, and Google Cloud).

It confirmed that the affected update has been pulled by ███████████.

CEO █████████ tweeted that “███████████ released an update that began impacting IT systems globally. We are aware of this issue and are working closely with ███████████ and across the industry to provide customers technical guidance and support to safely bring their systems back online”.

███████████ in a statement said the outage was not a result of a cyber-attack and they are actively working with customers impacted by a defect found in a single content update for Windows hosts. It had released a sensor configuration update to ███████████████. These updates were ongoing part of the protection mechanism of the Falcon Platform.

Customers running ██████ sensor for ███████████████ 7.11 and above that were online between Friday, July 19th 2024 (09:39 hours ███) and Friday July 19th 2024 (10:57 hours ███) may be impacted. Also, systems running ██████ sensor for Windows 7.11 and above that downloaded the updated configuration from 09:39 hours ███ to 10:57 hours ███ were susceptible to system crash.

They also clarified that configuration files referred to as “Channel files” are part of the behavioral protection mechanism used by ██████ sensor and are a normal part of sensor operations and occur several times a day in response to novel TTPs discovered by ███████████ and that this is not a new process. This configuration update triggered a logic error resulting in a system crash and blue screen of death (BSOD) on impacted suite.

Mac and Linux hosts are not impacted citing it is not a security incident or cyberattack. The issue had been identified, isolated and a fix has been deployed. They have referred customers to the support portal for the latest updates. They have further recommended organizations to ensure they’re communicating with ███████████ representatives through official channels. Therefore, ██████ is keeping a close watch on the situation for needful. Further updates will be provided as per need. ██████ representatives are also in touch with the ███████████ India team.

Conclusions:

This does not seem to be a cyber-attack as per the statement of █████████ and ███████████ and same has been echoed by counterpart agencies at CISA, USA; ████, UK, Australia and also the issue has also been mitigated globally and unlikely to have an impact beyond 72 more hours.

There is a business and commercial impact globally but India not been affected at global average. This seems to be because of the relatively less use of ███████████ products and less real time patching.

Overall this points to the need to diversify supply chain and managed service providers across the ecosystem while ensuing scrutiny for supply chain weaknesses. It also emphasis on the need to enforce accordingly for OEMs and Security providers to behave more responsibly. Ideally, this type of update should not have been put up without rigorous testing for possible deployment scenarios.

Annexures

Disruption have been reported to the below mentioned 11 Stock Broker entities:

1. ████████████████████
2. 5 paisa
3. 360 One
4. ████████████████████████
5. ███████████████████
6. ███████████████████████████████████
7. █████████████████████████████
8. Nuvama wealth and ███████████████
9. ██████████████
10. ███████████████████████
11. PhonePe Wealth Broking Pvt Ltd.