CIRT.GY Guyana National Computer Incident Response Team

AL2024_21 Impact of Faulty CrowdStrike Falcon Update

Description

A recent update to the CrowdStrike Falcon Sensor has caused significant disruptions to Windows systems globally. The faulty component has led to massive outages, impacting various organizations and services, including critical infrastructure such as airports, TV stations, and hospitals. This incident has highlighted the vulnerabilities and cascading effects of software issues within cybersecurity solutions. Guyana must take heed of these developments to bolster its own cybersecurity posture.

Details

On July 11, 2024, users worldwide began reporting issues with Windows hosts following the latest update to the CrowdStrike Falcon Sensor. A faulty Channel File within the update caused Windows systems to enter boot loops or display the Blue Screen of Death (BSOD). The following details outline the progression and impact of this incident:

Outage Timeline:

- The issue was first reported by users experiencing system crashes immediately after installing the update.
- CrowdStrike identified the faulty component, a Channel File, and rolled back the changes in subsequent updates.

Global Impact:

- Numerous large organizations across various sectors, including healthcare, aviation, and media, reported significant disruptions.
- Airports in major cities like Zurich, Melbourne, and New York experienced grounded flights and delays.
- Hospitals in the U.S., Canada, Spain, and the Netherlands faced operational challenges due to system outages.

Affected Systems:

- Windows workstations and servers were primarily impacted.

- Reports from companies indicated hundreds of thousands of computers were affected globally.

Remediation

In response to the incident, CrowdStrike issued several remediation steps to mitigate the impact of the faulty update. Organizations, including those in Guyana, should take the following actions to address the issue and prevent similar incidents:

Immediate Actions:

- Boot into Safe Mode: Restart Windows into Safe Mode or the Windows Recovery Environment.
- Remove Faulty File: Navigate to the C:\Windows\System32\drivers\CrowdStrike directory and delete the file matching “C-00000291*.sys”.
- Restart System: Boot the host normally to restore functionality.

For Cloud Environments:

- Detach and Backup: Detach the operating system disk volume from the impacted virtual server and create a backup.
- Delete Faulty File: Attach the volume to a new virtual server, navigate to the CrowdStrike directory, and delete the faulty file.
- Reattach Volume: Reattach the fixed volume to the impacted virtual server.

Long-term Measures:

- Update Communication Protocols: Ensure that all communication with CrowdStrike representatives is through official channels to receive timely updates and support.
- Review Update Policies: Implement stringent update policies to test new updates in a controlled environment before widespread deployment.
- Enhance Incident Response Plans: Strengthen incident response plans to quickly address and mitigate the impact of similar issues in the future.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Ilascu, I. (2024, July 19). CrowdStrike update crashes Windows systems, causes outages worldwide. Retrieved from *BleepingComputer*. https://www.bleepingcomputer.com/news/security/crowdstrike-update-crashes-windows-systems-causes-outages-worldwide/
- The Hacker News. (n.d.). *Faulty CrowdStrike update crashes Windows systems, impacting businesses worldwide*. Retrieved from The Hacker News https://thehackernews.com/2024/07/faulty-crowdstrike-update-crashes.html
- CrowdStrike. (2024, July 19). *Statement on Falcon content update for Windows hosts - Crowdstrike.com*. Crowdstrike.com. Retrieved from CrowdStrike. https://www.crowdstrike.com/blog/statement-on-falcon-content-update-for-windows-hosts/