مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Crowdstrike Outage and Potential System Crashes

Tracking #:432316071

Date:19-07-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a recent outage affecting Crowdstrike, a faulty update deployed by Crowdstrike is causing Windows systems running the Falcon sensor to crash with a blue screen of death (BSOD) error.

TECHNICAL DETAILS:

On July 19, 2024, CrowdStrike, experienced a significant global outage affecting numerous users. Reports indicate that many users were logged out of their systems and encountered critical errors, including the Blue Screen of Death (BSOD) on Windows devices.

Overview: A recent update from CrowdStrike has been causing Blue Screen of Death (BSOD) errors across multiple Microsoft Windows systems. This issue impacts system stability and can interrupt regular operations.

Affected Systems:

- Microsoft Windows (various versions)

Update from CrowdStrike:

- CrowdStrike has acknowledged the error and said “Our Engineers are actively working to resolve this issue and there is no need to open a support ticket.”
- CrowdStrike has released a temporary workaround to bring your device into an operable state, please note that this could disable your endpoint protection and as such enabling another endpoint protection tool such as defender would be advisable:

1. Boot Windows into Safe Mode or the Windows Recovery Environment.
2. Navigate to the C:\Windows\System32\drivers\CrowdStrike directory.
3. Locate the file matching "C-00000291* sys" file, right click and rename it to "C-00000291*.renamed*.
4. Boot the host normally.

RECOMMENDATIONS:

- Delay applying the recent Crowdstrike update until further notice and Rollback to Previous Version (if possible),Only if technically feasible and approved by your IT team, consider rolling back the Falcon sensor to the previous stable version to prevent further crashes.
- Identify Affected Systems that uses Crowdstrike Falcon on Windows systems.
- Monitor Crowdstrike Updates: Closely monitor Crowdstrike for updates and official communication regarding the outage and resolution.
- Testing Procedures: Establish testing procedures for security software updates before deploying them to production environments.
- Backup and Recovery: Maintain regular backups of your systems to facilitate recovery in case of incidents.
- Consider alternative security solutions for Windows systems while Crowdstrike resolves the issue.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.