THREAT BULLETIN

FA20240719-002 [Flash Alert] Exercise Caution: Threat Actors May Take Advantage Of Crowdstrike Outage

TLP
Clear

DESCRIPTION

Exercise Caution: Threat Actors May Take Advantage of Crowdstrike Outage

TLP:CLEAR = Recipients can spread this to the world, there is no limit on disclosure

Summary

On July 18th, CrowdStrike users experienced a significant issue wherein Windows workstations with the Crowdstrike Falcon sensor installed crashed and displayed the ominous blue screen of death (BSOD). This has led to significant outages worldwide as system admins race to apply the fixed update and get systems back online.

Given the current disruption, threat actors may take advantage of this global outage and reach out to IT administrators and/or end users and employ social engineering tactics, pretending to either be organizational IT helpdesk support OR Crowdstrike customer service representatives offering to “fix” their systems in attempt to gain access to business workstations. Threat actors may also share public links online or on social accounts prompting users to download malicious executables to install "quick fix" for this issue.

Users and system administrators are advised to exercise heightened caution when working to resolve outages associated with the defective software updates. Any users with questions regarding this outage should contact their IT departments at the official number and ask to speak to an administrator. Administrators as well should take caution only to speak with Crowdstrike customer support agents via known official channels.

References

https://therecord.media/crowdstrike-update-crashes-windows-devices-globally
https://www.crowdstrike.com/blog/statement-on-falcon-content-update-for-windows-hosts/

Reporting and Contact Information

In the event of a cybersecurity incident related to information found in this threat bulletin, Md. Code, Public Safety Article § 14-104.1 (c)(2) and Md. Code, State Finance & Procurement Article § 3.5-406(b)(2)) mandate that you report this via the Maryland Incident Reporting System. It is also recommended that you submit any shareable cyber threat intelligence to the MD-ISAC via the MD-ISAC Threat Intelligence Platform (TIP).

TLP:CLEAR = Recipients can spread this to the world, there is no limit on disclosure

TLP:CLEAR = Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information about Traffic Light Protocol (TLP) definitions and usage: https://www.cisa.gov/tlp