

**Computer Emergency Response Team of Mauritius  
Ministry of Information Technology, Communication and Innovation**

## **CERT-MU Security Alert**

**Date: 22 July 2024**

### **Update No 2: Microsoft Releases New Recovery Tool to Help with CrowdStrike Issue Impacting Windows Endpoints**

Microsoft has released a Recovery Tool to assist IT administrators in repairing Windows machines affected by CrowdStrike's faulty Falcon agent update, which crashed around 8.5 million devices last Friday. This tool generates a bootable USB drive, enabling IT admins to swiftly recover impacted systems. The recovery tool has 2 repair options:

1. Recover from Windows PE: this option uses boot media that automates the device repair.
2. Recover from safe mode: this option uses boot media for affected devices to boot into safe mode. An administrator can then sign in using an account with local administrative privileges and run the remediation steps.

To utilize the tool, users must have a 64-bit windows client with at least 8GB of free space and administrative privileges to create the bootable USB drive.

The tool can be downloaded from the Microsoft Download Center:

<https://go.microsoft.com/fwlink/?linkid=2280386>

---

**Date: 19 July 2024**

### **Update No 1: CrowdStrike Releases Workaround for the Blue Screen Error for Systems Running Microsoft Windows**

CERT-MU wishes to inform users that CrowdStrike has released a workaround to address the crashes on Microsoft Windows systems related to the Falcon Sensor. According to CrowdStrike, if hosts are still crashing and unable to stay online to receive Channel Files Changes, the following steps can be used to fix this issue:

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” and delete it.
4. Boot the host normally.

For more information about the update:

<https://supportportal.crowdstrike.com/s/article/Tech-Alert-Windows-crashes-related-to-Falcon-Sensor-2024-07-19>

---

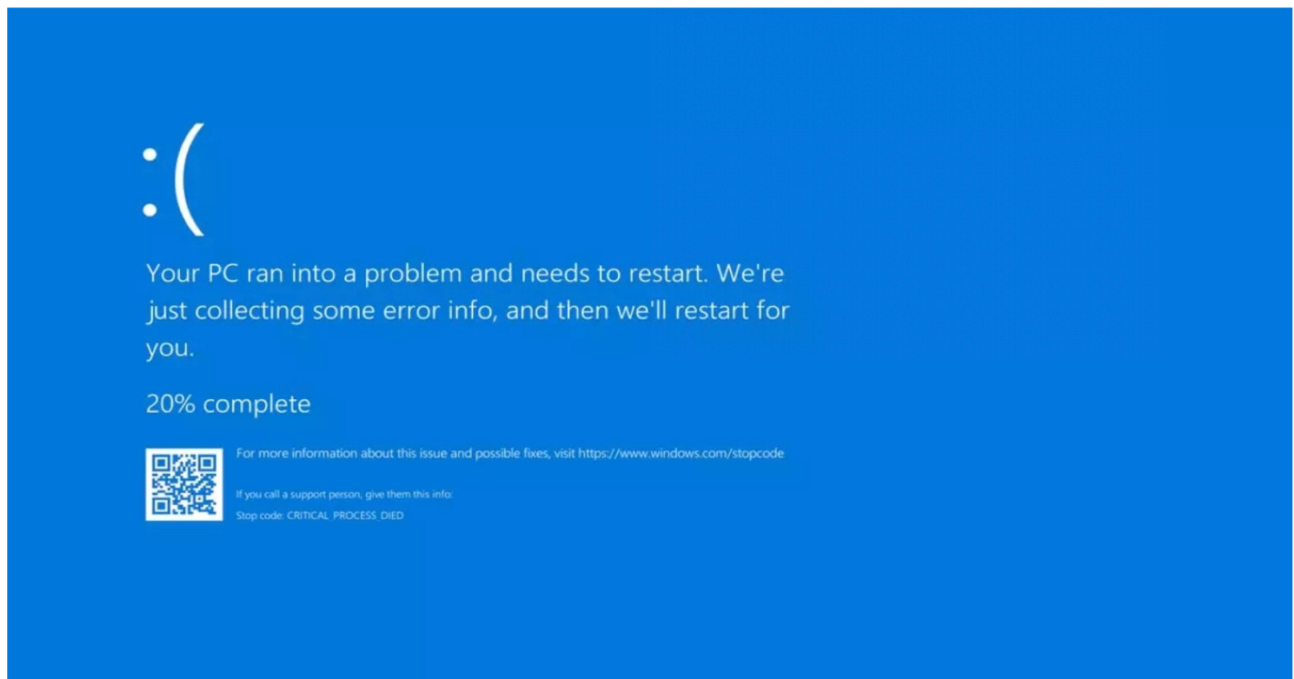
**Date of Issue: 19 July 2024**

**Severity: Critical**

## **Microsoft Windows PCs are Crashing Worldwide Due to CrowdStrike Issue**

### **Description**

Windows users around the world including Mauritius are experiencing involuntarily shut down of their PCs, along with the “Blue Screen of Death”, with the message that their Windows could not load. This issue is apparently caused because of an update by CrowdStrike to its Falcon software. Organisations around the world, including essential services in Australia, UK, US and Mauritius have already been impacted.



As per CrowdStrike, the company is aware of reports of crashes on Windows hosts related to the Falcon Sensor and they are trying to fix the issue. Potential workarounds along with a Technical Alert is expected to be published shortly. CERT-MU will post the updates as soon as they become available.

### **Report Cyber Incidents**

Report cyber security incident on the **Mauritian Cybercrime Online Reporting System (MAUCORS - <https://maucors.govmu.org/>)**

### **Contact Information**

**Computer Emergency Response Team of Mauritius (CERT-MU)**  
**Ministry of Information Technology, Communication and Innovation**

Tel: 460 3010

Hotline No: (+230) 800 2378

Gen. Info. : [contact@cert.govmu.org](mailto:contact@cert.govmu.org)

Incident: [incident@cert.govmu.org](mailto:incident@cert.govmu.org)

Website: <https://cert-mu.govmu.org/>

MAUCORS: <https://maucors.govmu.org/>