

Subject: **Cyber Security Advisory – Windows Outage Affecting Version 10 and 11 Globally (Advisory No. 16)**

Introduction. A recent update to CrowdStrike’s Falcon sensor has caused significant disruptions for Windows 10 and 11 users globally, leading to Blue Screen of Death (BSOD) loops and rendering systems inoperable. Users report repeated BSODs with the error message DRIVER_OVERRAN_STACK_BUFFER, preventing normal system boot and operation.

2. **Incident Details.** The impact has been particularly severe to large enterprises (banks, airlines, hospitals, broadcasters etc.), with some organizations reporting thousands of affected devices, including critical production servers.

3. **Recommendations.** Above in view, to safeguard against Windows outage issue, users are advised to ensure backup and high availability of critical services/data/systems as a contingency measure. Moreover, in order to specifically resolve above mentioned issue, users/administrators are advised to perform following steps:

- a. Boot windows into safe mode or the windows recovery environment
- b. Navigate to this directory: C:\Windows\System32\Drivers\CrowdStrike
- c. Locate the file matching C-00000291*.sys and delete this file
- d. Finally, boot the windows normally after removing above mentioned file
- e. CrowdStrike fix may be applied on test environment and on successful test-run (24 hours) may be deployed on production systems