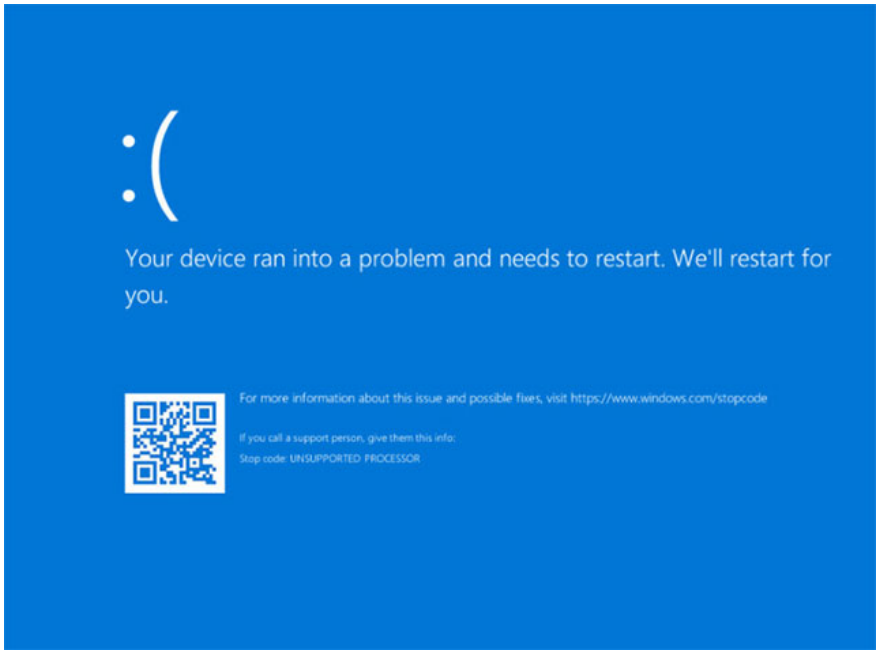
CrowdStrike also crippled global Debian and Rocky Linux systems many months ago, but no one noticed!

CrowdStrike is a large cybersecurity company headquartered in the US, operating mainly in the field of providing defense software services and risk management against cyber attacks and malware at the enterprise level. .

The biggest 'drama' in the technology world in the past few hours is probably the 'blue screen of death' (BSOD) incident on Windows PCs, which has disrupted the operations of many different fields, especially photography. affecting airlines, banks and medical services worldwide for hours on end. Preliminary assessment results show that the problem is caused by a problematic file delivered via an update from the world's leading cloud cybersecurity service provider CrowdStrike. CrowdStrike later confirmed that the issue did not affect Mac or Linux PCs, but only Windows users.

CrowdStrike is a large cybersecurity company headquartered in the US, operating mainly in the field of providing defense software services and risk management against cyber attacks and malware at the enterprise level. . However, the incident on July 19 was caused by the company's own software, causing millions of computers worldwide to become inoperable, severely affecting the operations of hundreds of thousands of companies.



Although many people may consider this an isolated incident, in fact, CrowdStrike a few months ago also caused similar problems on some Linux platforms, just due to a much smaller user base. Compared to Windows, not many people care.

In fact, Debian and Rocky Linux users also recently experienced significant disruption due to CrowdStrike updates, raising serious concerns about the company's software update and testing process.

Accordingly, in April, a CrowdStrike update caused all Debian Linux servers in a civilian technology lab in the United States to crash simultaneously and refuse to boot. The update appears to be incompatible with the latest stable version of Debian, although the Linux configuration is said to support it. The lab's IT team initially didn't know what was causing the problem, but then accidentally discovered that removing CrowdStrike had allowed the machine to boot, and immediately reported the incident.

A member of the IT team involved in the incident expressed dissatisfaction with CrowdStrike's delayed response. It took them weeks to find the root cause after admitting the problem a day later. Analysis shows that Debian Linux configurations are not included in CrowdStrike's testing matrix. Instead, the company simply 'pushes' the software onto the partner's computer system.

This is not an isolated incident. CrowdStrike users also reported similar issues after upgrading to RockyLinux 9.4, causing their servers to crash due to a kernel error. The Crowdstrike support team has acknowledged this issue, highlighting an incomplete and unanticipated testing model for compatibility issues across various operating systems.

To avoid similar issues in the future, CrowdStrike should prioritize rigorous testing on all supported configurations. Additionally, organizations should approach the CrowdStrike update with caution and have a contingency plan in place to minimize potential disruptions.