Statement on major IT outage

Following the global IT outage on Friday 19 July, affected organisations should put in place vendor mitigations. The NCSC is also warning about an increase in related phishing.

A widely reported IT outage following a CrowdStrike security update has today caused significant global disruption. The NCSC assesses that the outages are not the result of a security incident or malicious cyber activity.

What should I do?

Fixes are now available to resolve the issues, and affected organisations should refer to the relevant vendor guidance and take the necessary action.

Installing security updates is still an essential security practice and organisations should continue to install them when they are available. Organisations should also continue to use antivirus products as normal.

Increase in phishing

Note that an increase in phishing referencing this outage has already been observed, as opportunistic malicious actors seek to take advantage of the situation. This may be aimed at both organisations and individuals.

Organisations should review NCSC guidance to make sure that multi-layer phishing mitigations are in place, while individuals should be alert to suspicious emails or messages on this topic and know what to look for.

Future readiness

Incidents such as this global outage can have a huge impact on your organisation. The NCSC's incident response guidance is a good place to begin.

PUBLISHED

19 July 2024

NEWS TYPE

Statement