



Security updates released for Microsoft Exchange Servers

The National Cyber Security Centre (NCSC) is encouraging organisations to install critical updates following a number of vulnerabilities being addressed in Microsoft Exchange.

As part of Microsoft's scheduled April update cycle, a number of critical severity vulnerabilities were addressed in Microsoft Exchange. NCSC have no information to suggest that these vulnerabilities are being used in active exploitation. However, given the recent focus on Exchange, NCSC recommend the installation of updates as soon as practicable, as attackers may seek to build exploit capability which could be used against systems before the updates are applied.

The vulnerabilities affect Microsoft Exchange Server. The affected versions are:

- Exchange Server 2013
- Exchange Server 2016
- Exchange Server 2019

Organisations running an out-of-support version of Microsoft Exchange should update to a supported version without delay.

Exchange Online customers are already protected.

Recommendation

The NCSC recommends following vendor best practice advice in the mitigation of vulnerabilities. In this case, the most important aspect is to install the latest security updates immediately. The April 2021 security update fixes a number of security vulnerabilities and [more information can be found on Microsoft's website](#).

More information on [installing these updates is available in Microsoft's Exchange blog](#).

Further Information

NCSC advise that if organisations are unsure about how to update or uncertain whether updates have installed successfully, please refer to the Microsoft support documents. If organisations are unsure about whether they have affected servers, or are unsure of the update status, consult the Microsoft Exchange Server Health Checker.

For more information on how to keep safe online visit [NCSC](#) and [Cyber Aware](#).

You can report suspicious emails by forwarding the original message to the Suspicious Email Reporting Service (SERS) at report@phishing.gov.uk

If you receive a suspicious text you can forward this to 7726 which spells SPAM on your phone keypad.

If you have been a victim of crime, and it is not an ongoing emergency, you can report this to Police Scotland on 101. For all emergency calls, dial 999.

*This alert was sent out for your information by Police Scotland
Cybercrime Harm Prevention Unit - PPCWCyberHarmPrevention@scotland.pnn.police.uk
All information was correct at time of distribution. 14/04/2021*