NEWS

Microsoft vulnerabilities exploitation - updated advice

Urgent updates and actions following Exchange server vulnerabilities

> This alert is an updated version of the NCSC alert from 3 March 2021 and contains additional information on installing updates and detection.

On 2 March 2021 Microsoft made public that sophisticated actors had attacked a number of Exchange servers. In response to this they released multiple security updates for affected servers. This does not affect Exchange Online.

The updates were released ahead of the monthly update cycle because four of the seven vulnerabilities have been used in ongoing attacks. The security updates fix the vulnerabilities exploited in the attack.

A wide variety of threat actors are using automated tools to scan for Exchange servers where updates are not installed. The actors then install malicious software to servers identified as vulnerable. On 11 March it was reported that ransomware actors have also exploited these vulnerabilities, or made use of the installed malicious software, to install ransomware on a network.

Affected versions

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

- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016

- Microsoft Exchange Server 2019

A defence in depth update for Microsoft Exchange Server 2010 has also been released. Organisations running an out-of-support version of Exchange Server should update to a supported version **without delay**.

Exchange Online (as part of Microsoft 365) is **not** affected.

Recommended priority actions (updated 12 March)

1. **Install the latest updates immediately**
   This should be the first priority for all UK organisations using affected versions of Microsoft Exchange Server.
   - Security updates can be found on the Microsoft website.
   - Microsoft has produced an additional series of security updates that can be applied to some older (and unsupported) Cumulative Updates (CUs). This is intended only as a temporary measure to protect vulnerable servers right now. Organisations still need to update to the latest supported CU and then apply the applicable security updates.
   - 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.

2. **If updates cannot be installed, the recommended Microsoft mitigations should be implemented**
   - These mitigations are temporary measures and only recommended where updating is not immediately possible.

3. **If organisations cannot install the updates, or apply any of the mitigations, the NCSC recommends isolating the Exchange server from the internet by:**
   - Blocking untrusted connections to the Exchange server port 443
   - If secure remote access solutions are already in place (such as a VPN or VDI), configuring Exchange only to be available remotely via this solution.

4. **The NCSC strongly advises all organisations using affected versions of Microsoft Exchange Servers to proactively search systems for evidence of compromise, in line with Microsoft guidance linked below**

This advice applies irrespective of update status because a compromise may have occurred before updates were installed and installing the update will not remediate a previous compromise.

Further information regarding indicators of compromise and detection can be found below:

- In the Microsoft guidance
- CISA and the FBI in the US have published a TLP WHITE advisory
- Exchange server hash list
- Microsoft Exchange On-premises Mitigation Tool (EOMT) automatically downloads any dependencies, mitigates against current known attacks using CVE-2021-26855 and runs the Microsoft Safety Scanner

If organisations identify activity of concern, they should consider whether to engage with an IR company using standard organisational incident response processes.

Reporting a compromise

Affected UK organisations should report any suspected compromises to the NCSC via the website.

PUBLISHED

12 March 2021

NEWS TYPE

Alert

WRITTEN FOR

Small & medium sized organisations

Large organisations

Public sector

Was this article

Was this article helpful?

Yes No