National Cyber Security Centre

# Cyber Security Advisory

CSA-2021-2291

The National Cyber Security Centre is hosted within the Government Communications Security Bureau

**14 April 2021**

The Traffic Light Protocol (TLP) marking is used to ensure that sensitive information is shared with the correct audience. Subject to standard copyright rules, **TLP: WHITE** information may be distributed without restriction.

The severity rating for this Cyber Security Advisory is **HIGH**. This indicates the NCSC has identified activity which may pose an immediate threat to the confidentiality, integrity or availability of your IT systems. NCSC recommends any remedial actions outlined in this report are expedited to prevent or mitigate the risk associated with this activity.

## Critical vulnerabilities affecting on premise Microsoft Exchange servers

### Overview

The National Cyber Security Centre (NCSC) is aware of multiple critical vulnerabilities affecting on premise Microsoft Exchange servers. Microsoft has released patches for these vulnerabilities as part of the April 2021 patch-Tuesday release. These vulnerabilities are unrelated to earlier Exchange vulnerabilities, made public in early March 2021.

Microsoft has released a security advisory[1] detailing these vulnerabilities, which include the ability for an unauthenticated actor to execute remote code on vulnerable hosts. The NCSC strongly recommends organisations running affected instances of Microsoft Exchange Server apply the security patches as soon as possible.

The vulnerabilities affect the following versions of Microsoft Exchange Server:

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

[1] https://msrc-blog.microsoft.com/2021/04/13/april-2021-update-tuesday-packages-now-available/

Successful exploitation of these vulnerabilities could allow an actor to gain remote code execution with elevated privileges on the impacted device. This can facilitate the deployment of malware to enable continued access to the compromised system, even after the system has been patched.

The NCSC has no information to suggest that these vulnerabilities are being actively exploited in New Zealand. The vulnerabilities are being tracked as the following CVEs:

- CVE-2021-28480 - Microsoft Exchange Server Remote Code Execution Vulnerability
- CVE-2021-28481 - Microsoft Exchange Server Remote Code Execution Vulnerability
- CVE-2021-28482 - Microsoft Exchange Server Remote Code Execution Vulnerability
- CVE-2021-28483 - Microsoft Exchange Server Remote Code Execution Vulnerability

Microsoft Exchange Online is not known to be affected by these vulnerabilities.

While there is no information available that indicates these vulnerabilities have been exploited, the NCSC is aware of multiple actors exploiting previously identified Exchange vulnerabilities that were patched by Microsoft in March 2021.

Actors often reverse-engineer patches to identify and exploit vulnerabilities, as such, the NCSC recommends organisations apply security patches as soon as possible.

## Recommendations

The NCSC strongly recommends organisations running affected instances of Microsoft Exchange Server apply the security patches as soon as possible.

Please contact the NCSC if you identify evidence of malicious activity within your network.

*The NCSC can be contacted by email via **incidents@ncsc.govt.nz** or phone **(04) 498 7654***
*We encourage you to contact us at any time if you require any further assistance or advice.*