NCSC

National Cyber Security Centre

2111101000-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Microsoft November 2021 Security Updates
2021-11-10

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

Microsoft has released details of 55 security patches for software, including patches for some zero-day vulnerabilities, which have been actively exploited in the wild.

System administrators should refer to Microsoft documentation on these vulnerabilities and apply patches as appropriate. Details of the November 2021 release can be found at the following link: November 2021 Release Notes.

The NCSC would like to highlight two of these vulnerabilities as they have been actively exploited in the wild and it is believed that more widespread exploitation will occur in the near future.

- **CVE-2021-42321** - Microsoft Exchange Server Remote Code Execution Vulnerability (CVSS 8.8) This is a post-authentication vulnerability in Exchange Server. In order to check if exploit was previously attempted, Microsoft have advised administrators to run the following PowerShell query on Exchange servers to check for specific events in the Event Log:

  ```
  Get-EventLog -LogName Application -Source "MSExchange Common" -EntryType Error
  | Where-Object { $_.Message -like "*BinaryFormatter.Deserialize*" }
  ```

  If events are found, further analysis and incident response procedures should be initiated.

- **CVE-2021-42292** - Microsoft Excel Security Feature Bypass Vulnerability (CVSS 7.8), this vulnerability was found in Microsoft Excel and can be used to circumvent security controls. Microsoft says that the Preview Pane is not an attack vector.

Products Affected

A range of Microsoft Products are affected in this security update. Details of these products can be found here.
With regard to CVE-2021-42321, the following versions of Microsoft Exchange are affected:

- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019

It is recommended that systems are kept up to date with the latest patches.

Impact

There are multiple possible impacts that may occur across the vulnerabilities listed including Remote Code Execution and Elevation of Privilege.

Recommendations

The NCSC recommends that affected organisations apply the security updates from Microsoft as a matter of urgency, Figure 1 below, shows Microsoft's recommended update path for Exchange Server:

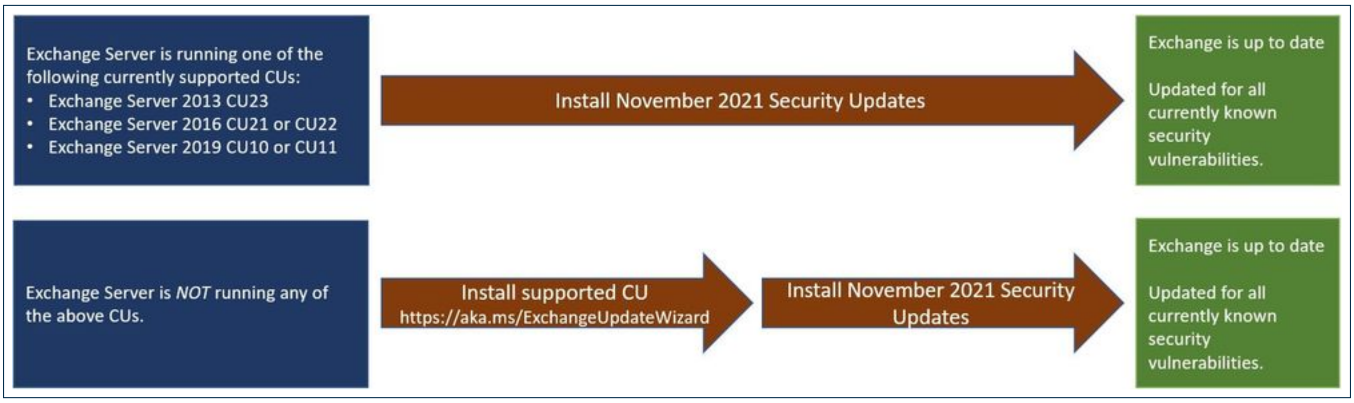
Exchange Server is running one of the following currently supported CUs:
• Exchange Server 2013 CU23
• Exchange Server 2016 CU21 or CU22
• Exchange Server 2019 CU10 or CU11
Install November 2021 Security Updates
Exchange is up to date
Updated for all currently known security vulnerabilities.
Exchange Server is *NOT* running any of the above CUs.
Install supported CU
https://aka.ms/ExchangeUpdateWizard
Install November 2021 Security Updates
Exchange is up to date
Updated for all currently known security vulnerabilities.

Figure 1: Update Path Options

Microsoft have also highlighted an issue that Exchange 2013 CU23 customers who use Windows Server Update Services (WSUS) to download Security Updates might see an error with the installation of November SU (error 0x80070643 in the event log, event ID 20).

The NCSC would again re-iterate the importance for organisations to ensure all software is kept up to date.

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie