National Cyber Security Centre

21090801000-NCSC

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

NCSC Alert

Microsoft Exchange ProxyShell Vulnerability - UPDATE 08-09-2021

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.*

Revision History

Revision	Date	Author(s)	Description
1.0	09 August 2021	CSIRT-IE	Initial Alert created regarding Microsoft Exchange Vulnerabilities known as ProxyShell (https://www.ncsc.gov.ie/pdfs/MS_Proxyshell_090821.pdf)
1.1	08 September 2021	CSIRT-IE	Additional information added regarding compromise of vulnerable servers prior to patching. Also, TTPs used by attackers

ProxyShell Vulnerability

Threat Type	The NCSC has observed on-going exploitation of the vulnerabilities known as **ProxyShell**, targeting vulnerable instances of Microsoft Exchange. **This updated Alert is being published to remind organisations to apply patches in a timely manner. If you have applied the patches as recommended in August 2021, we would like to highlight the importance of carrying out investigative analysis to determine if Microsoft Exchange servers were compromised prior to patching the vulnerabilities below.** The NCSC estimate that circa **40% of internet facing Microsoft Exchange servers in Ireland** are potentially still vulnerable to this particular threat. **ProxyShell**, discovered by the security researcher Orange Tsai, is the name for three vulnerabilities that perform unauthenticated, remote code execution on Microsoft Exchange servers when chained together. The three vulnerabilities are: • CVE-2021-34473 - Pre-auth Path Confusion leading to ACL Bypass. • CVE-2021-34523 - Elevation of Privilege on Exchange PowerShell Backend. • CVE-2021-31207 - Post-auth Arbitrary-File-Write leading to RCE. When chained together, these vulnerabilities allow an unauthenticated attacker to remotely execute arbitrary commands as SYSTEM.
Products Affected	The following versions of Microsoft Exchange are affected (if they have not already been updated with the May 2021 Cumulative Update KB5003435). • Microsoft Exchange Server 2013 • Microsoft Exchange Server 2016 • Microsoft Exchange Server 2019 It is recommended that systems are kept up to date with the latest patches.
Impact	Remote Code Execution - compromised systems and data loss. The NCSC has observed further payloads being installed on target systems such as webshells, cryptocurrency miners, backdoors and Ransomware.

TTPs	The NCSC has observed the following Tactics, Techniques and Procedures being used in attacks against Microsoft Exchange Servers:
	
	ASPX files that are dropped in specific folders are not true aspx files but rather Microsoft Outlook email folders.
	
	`file QSGVRWMWXQXARG.aspx`
	`QSGVRWMWXQXARG.aspx: Microsoft Outlook email folder (>=2003)`
	
	Webshells have been found deployed in the following directories:
	• C:\inetpub\wwwroot\aspnet_client\
	• C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy \owa\auth\
	• We have also observed directories created in the C:\ProgramData directory, these directories have been observed named, **XYZ, COM, COM1, WHO, ZING & ZOO**
	• New virtual directories have been observed being created in the C:\Windows\System32\inetsrv\Config\applicationHost.config file.
	• Some webshells have been observed copied to the C:\Users\All Users folder also.

Recommendations	The NCSC recommends that affected organisations update Microsoft Exchange server as soon as possible. Microsofts advice regarding this threat can be found here. You can check if your Microsoft Exchange instance is affected by reviewing your Exchange Server's IIS logs for the "**/autodiscover/autodiscover.json**" or "**/mapi/nspi/**" strings. If the results list the targeted Autodiscover URL, then threat actors scanned your server for the vulnerability. In relation to the C:\Windows\System32\inetsrv\Config\applicationHost.config file. Administrators should check for the presence of new paths and examine any newfound paths to find and remove webshells. Also remove the edited lines in the applicationHost.config. **UPDATE:** Patching will provide protection from future exploitation of this vulnerability, however the NCSC advises that affected organisations **review the TTPs/ Recommendations section of this alert and search for any evidence of post-compromise activity on affected systems**. Sigma rules to detect ProxyShell exploitation attempts: • HTTP log • Process Creation Yara Rules to detect ProxyShell exploitation can be found at the following link: • Signature base Yara rules for ProxyShell

MITRE Att&ck

- Reconnaissance
  - Active Scanning: Vulnerability Scanning (T1595.002)
- Initial Access
  - Exploit Public-Facing Application (T1190)
- Execution
  - System Services (T1569)
  - Command and Scripting Interpreter (T1059)
- Persistence
  - Create Account (T1136)
  - Server Software Component: Web Shell (T1505.003)
  - Account Manipulation: Exchange Email Delegate Permissions (T1098.002)
- Privilege Escalation
  - Exploitation for Privilege Escalation (T1068)
- Discovery
  - File and Directory Discovery (T1083)
  - Network Service Scanning (T1046)
  - Remote System Discovery (T1018)
- Lateral Movement
  - Remote Services (T1021)
- Command & Control
  - Application Layer Protocol (T1071)

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