National Cyber Security Centre

2108090847-NCSC

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

NCSC Alert

Microsoft Exchange ProxyShell Vulnerability
2021-08-09

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.*

Threat Type	The NCSC has been made aware that threat actors are actively scanning for the Microsoft Exchange ProxyShell RCE vulnerability. 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
Impact	Remote Code Execution - compromised systems, data loss.
Recommendations	The NCSC recommends that affected organisations update Microsoft Exchange server as soon as possible. Further details on the May cumulative update for Microsoft Exchange Server can be found here. A further check can be performed to check if your version of Exchange 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. Sigma rules to detect ProxyShell exploitation attempts: • HTTP log • Process Creation

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