NCSC
National Cyber Security Centre

2209301000-NCSC

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

NCSC Alert

Microsoft Exchange Server - Zero-Day Vulnerabilities CVE-2022-41040, CVE-2022-41082

30 September 2022

Status: TLP-WHITE

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-WHITE *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-WHITE *information may be shared 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

Vietnamese Cyber security company, GTSC, has identified two Zero-Day vulnerabilities affecting Microsoft Exchange Server 2013, 2016, and 2019.

- **CVE-2022-41040**: Server-Side Request Forgery (SSRF) vulnerability, which enables an authenticated attacker to remotely trigger CVE-2022-41082.
- **CVE-2022-41082**: Remote Code Execution (RCE) when PowerShell is accessible to the attacker.

Microsoft Exchange Online Customers do not need to take any action. On premises Microsoft Exchange customers should review and apply the advice which is contained in the following Microsoft blog:
https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/

Attempts to exploit these vulnerabilities have been observed in the wild and as there is currently no patch available, the NCSC recommend that organisations implement the workarounds as a matter of urgency.

As new information becomes available this advisory will be updated.

Products Affected

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

Impact

Remote Code Execution, Server Side Request Forgery, Access to sensitive data

Recommendations

These vulnerabilities are similar to the Proxyshell vulnerabilities that were published and widely exploited last year.

The NCSC recommends that affected organisations apply the workarounds which are contained in the Microsoft Blog as soon as possible. When a patch becomes available, it should be installed as a matter of urgency.

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
LinkedIn: ncsc-ie