National Cyber Security Centre

2402140126-NCSC

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

# NCSC Alert

## Critical Vulnerability exists in Microsoft Outlook 2016 (CVE-2024-21413)

Wednesday 14th February, 2024

**STATUS:** TLP-CLEAR

*Recipients can spread this to the world, there is no limit on disclosure. Sources may use* TLP-CLEAR *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-CLEAR *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

**Published:** 2024-02-13T18:16:00
**Vendor:** Microsoft
**Product:** Microsoft Outlook 2016
**CVE ID:** CVE-2024-21413
**CVSS 3.0 Score**[1]**:** 9.8
**EPSS**[2]**:** N/A
**Summary:** Microsoft Outlook Remote Code Execution Vulnerability

Microsoft has released an update for Microsoft Office 2016 which patches a critical vulnerability within Microsoft Outlook 2016. The vulnerability, CVE-2024-21413, has a CVSS 3.0 score of 9.8.

## Products Affected

- Microsoft Office 2016 (32 & 64 bit)

## Impact

The Common Weakness Enumeration (CWE)[3] type of this vulnerability is Remote Code Execution (RCE). Exploitation of this vulnerability allows an attacker to bypass the Office Protected View and execute code in Edit mode. If successful, the attacker could gain high privileges on the system by sending a maliciously crafted link.

This vulnerability is currently not present in CISA Known Exploited Vulnerability (KEV) catalog[4]

## Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from Microsoft.

Additional recommendations and mitigations for CVE-2024-21413 can be found in the respective link: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21413

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://www.first.org/epss/articles/prob_percentile_bins
[3] https://cwe.mitre.org/
[4] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

**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@ncsc.gov.ie
**Web:** ncsc.gov.ie
**Twitter:** ncsc_gov_ie
**LinkedIn:** ncsc-ie