National Cyber Security Centre

[2407110151]-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical vulnerability exists in Microsoft Office - CVE-2024-38021

Thursday 11th July, 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: 2024-07-09T17:15:00
Vendor: Microsoft
Product: Microsoft Office (various versions)
CVE ID: CVE-2024-38021
CVSS3.1 Score[1]**:** 8.8
EPSS[2]**:** 0.470070000
(For up to date EPSS score, click here: https://api.first.org/data/v1/epss?cve=CVE-2024-38021
Summary: Microsoft Outlook Remote Code Execution Vulnerability

Products Affected

- Microsoft Office 2019 affected from 19.0.0
- Microsoft 365 Apps for Enterprise affected from 16.0.1
- Microsoft Office LTSC 2021 affected from 16.0.1
- Microsoft Office 2016 affected from 16.0.0

Impact

CVE-2024-38021 is a high-severity vulnerability affecting Microsoft Outlook where an attacker could craft a malicious link that bypasses the Protected View Protocol, which could lead remote code execution (RCE) allowing them to gain high privileges, which include read, write, and delete functionality.

Common Weakness Enumeration (CWE)[3]**:** CWE-20: Improper Input Validation

Present in CISA Known Exploited Vulnerability(KEV)[4] **catalog:** NO
Used by Ransomware Operators: Not Known

Recommendations

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

Additional recommendations and mitigation's for CVE-2024-38021 can be found in the respective link(s) below: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38021

[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
Tom Johnson House,
Beggars Bush,
Dublin, D04 A068,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre