NCSC
National Cyber Security Centre

2312130112-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerability exists in Microsoft Windows (CVE-2023-35628)

Thursday 14th December, 2023

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: 2023-12-12T18:15:00
Vendor: Microsoft
Product: Multiple versions of Microsoft Windows
CVE ID: CVE-2023-35628
CVSSv3.0 Score: 8.1

Summary: Windows MSHTML Platform Remote Code Execution Vulnerability.

More information related to this issue can be found at the following link(s):
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35628

Products Affected

- Windows 11 Version 23H2
- Windows 11 version 22H3
- Windows Server 2022, 23H2 Edition (Server Core installation)
- Windows 10 Version 1809
- Windows Server 2019
- Windows Server 2019 (Server Core installation)
- Windows Server 2022
- Windows 11 version 21H2
- Windows 10 Version 21H2
- Windows 11 version 22H2
- Windows 10 Version 22H2
- Windows 10 Version 1507
- Windows 10 Version 1607
- Windows Server 2016
- Windows Server 2016 (Server Core installation)
- Windows Server 2008 R2 Service Pack 1
- Windows Server 2008 R2 Service Pack 1 (Server Core installation)
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)

Impact

Common Weakness Enumeration (CWE): Remote Code Execution

Present in CISA Known Exploited Vulnerability(KEV) catalog: NO

Recommendations

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

Additional recommendations and mitigation's for the CVE can be found in the respective links below: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35628

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