National Cyber Security Centre

2408140157-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Microsoft Vulnerabilities including Windows TCP/IP Remote Code Execution Vulnerability

Wednesday 14th August, 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: 2024-08-13T18:15:00
Vendor: Microsoft
Product: Security updates have been released for Microsoft products. Of the vulnerabilities fixed, several have been classified as critical.

The critical vulnerability CVE-2024-38063, which would affect the TCP/IP stack when IPv6 is enabled, and whose successful exploitation would allow remote code execution (RCE) on the affected system. Microsoft has rated this vulnerability as “most likely to exploit” and has been assigned a CVSSv3 score of 9.8.

Microsoft also published details of several other critical zero-day vulnerabilities which are detailed below that are being actively exploited.

Products Affected

CVE-2024-38063 (CVSS:3.1 Score:9.8)
CVE-2024-38178 (CVSS:3.0 Score:7.5)
CVE-2024-38106 (CVSS:3.0 Score:7)
CVE-2024-38213 (CVSSv3.0 Score:6.5)
CVE-2024-38193 (CVSSv3.0 Score:7.8)

- Windows Server 2022
- Windows Server 2022, 23H2 Edition (Server Core installation)
- Windows Server 2019
- Windows Server 2019 (Server Core installation)
- Windows Server 2016
- Windows Server 2016 (Server Core installation)
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2008 Service Pack 2
- Windows Server 2008 Service Pack 2 (Server Core installation)
- Windows Server 2008 Service Pack 2
- Windows Server 2008 R2 Service Pack 1
- Windows Server 2008 R2 Service Pack 1 (Server Core installation)
- Windows 11 Version 24H2
- Windows 11 Version 23H2
- Windows 11 version 22H3
- Windows 11 version 22H2
- Windows 11 version 21H2
- Windows 10 Version 22H2
- Windows 10 Version 21H2
- Microsoft Windows 10 Version 1809
- Windows 10 Version 1607
- Windows 10 Version 1507

CVE-2024-38109 (CVSS:3.1 Score:9.1)

- Microsoft Azure Health Bot

CVE-2024-38189 (CVSS:3.1 Score:8.8)

- Microsoft Project

CVE-2024-38206 (CVSS:3.1 Score:8.5)

- Microsoft Copilot Studio

Impact

CVE-2024-38063

- Remote code execution on the affected system

CVE-2024-38109

- Elevation of Privilege Vulnerability

CVE-2024-38189

- Remote code execution on the affected system (Actively exploited)

CVE-2024-38206

- Information Disclosure Vulnerability

CVE-2024-38178

- Scripting Engine Memory Corruption Vulnerability(Exploited)

CVE-2024-38106

- Windows Kernel Elevation of Privilege Vulnerability(Exploited)

CVE-2024-38213

- Windows Mark of the Web Security Feature Bypass Vulnerability(Exploited)

CVE-2024-38193

- Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability(Exploited)

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from Microsoft. More information can be found here:
https://msrc.microsoft.com/update-guide/releaseNote/2024-Aug

Additional recommendations and mitigations for these CVEs can be found in the respective link(s) below:
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38189
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38206
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38109
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38178
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38106
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193

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