National Cyber Security Centre

2303150112-NCSC

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

NCSC Alert

Microsoft Outlook, Windows SmartScreen zero-day vulnerabilities - CVE-2023-23397, CVE-2023-24880

Thursday 16th March, 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

As part of their regular patching cycles, Microsoft have released patches to address two zero-day vulnerabilities that exist within their Outlook for Windows and Windows SmartScreen products. Both of these zero-days have been actively exploited in the wild.

- A zero-day vulnerability in Microsoft Outlook for Windows that allows Elevation of Privilege (EoP) through NTLM credential theft, allowing an attacker to authenticate as the victim. The vulnerability is tracked as CVE-2023-23397 and classified as 'critical' with a CVSS score of 9.8.
- An actively exploited zero-day vulnerability is in Windows SmartScreen that can be used to create executables that bypass the Windows Mark of the Web(MOTW) security warning. The vulnerability is tracked as CVE-2023-24880. This CVE is likely used in a chain attack and has been linked to a number of ransomware campaigns, with a notable focus on Europe.

More information can be found in Microsoft's security update guides:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-24880

In addition, a number of critical and high rated vulnerabilities have also been addressed in the March Patch Tuesday release. Please see the Recommendations section below for further information.

Products Affected

CVE-2023-23397: All supported versions of Microsoft Outlook for Windows are affected. Other versions of Microsoft Outlook such as Android, iOS, Mac, as well as Outlook on the web and other M365 services are not affected.

CVE-2023-24880: All desktop systems running Windows 10 and above and systems running Windows Server 2016, 2019, and 2022.

Impact

CVE-2023-23397: Exfiltration of victim emails and other confidential data linked to their Outlook Accounts.

CVE-2023-24880: Loss of integrity to Smartscreen and Protected View services, allowing the propagation of malware with greater ease.

Recommendations

CVE-2023-23397: The NCSC strongly advises affected organisations to follow Microsoft's advice and update Microsoft Outlook for Windows to remain secure. To determine if your organization was targeted by actors attempting to use this vulnerability, Microsoft provides documentation and tools here:

CVE-2023-24880: The NCSC strongly advises to apply the updates per Microsoft's security update guides instructions.

Microsoft has also addressed five critical remote code execution (RCE) vulnerabilities in its latest security guide. At the time of writing, there have been no reports of active exploitation of these vulnerabilities in the wild. Details of these including mitigation actions can be found here:

- CVE-2023-21708 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
- CVE-2023-23392 - HTTP Protocol Stack Remote Code Execution Vulnerability
- CVE-2023-23404 - Windows PPTP Remote Code Execution Vulnerability
- CVE-2023-23415 - Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability
- CVE-2023-23416 - Windows Cryptographic Services Remote Code Execution Vulnerability

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