Security Advisory 2023-009

Multiple Critical Vulnerabilities in Microsoft Products

February 15, 2023 — v1.0

TLP:CLEAR

History:

- *15/02/2023 — v1.0 – Initial publication*

Summary

On February 14, Microsoft released its February 2023 Patch Tuesday advisory disclosing 79 vulnerabilities (with 9 critical ones), including 3 exploited zero-day vulnerabilities identified with `CVE-2023-21823`, `CVE-2023-21715` and `CVE-2023-23376`, which affect respectively Windows Graphics Component, Microsoft Publisher and Windows Common Log File System Driver [1].

Microsoft patched additional three remote code execution Exchange Server flaws (CVE-2023-21706, CVE-2023-21707, and CVE-2023-21529) that are likely to be exploited, but an authentication is required.

It is highly recommended to patch affected devices.

Technical Details

CVE-2023-21823 - Windows Graphics Component Remote Code Execution Vulnerability [2]

This vulnerability, with a CVSS score of 7.8 out of 10, affects the Windows Graphics Component and could allow an attacker to execute commands with SYSTEM privileges.

This security update will be pushed out to users via the Microsoft Store rather than Windows Update. Therefore, for those customers who disable automatic updates in the Microsoft Store, Microsoft will not be pushing out the update automatically.

CVE-2023-21715 - Microsoft Publisher Security Features Bypass Vulnerability [3]

This vulnerability, with a CVSS score of 7.3, affects Microsoft Publisher and allows a specially crafted document to bypass Office macro policies that block untrusted or malicious files. Exploiting this flaw would effectively allow macros in a malicious Publisher document to run without first warning the user.

The attack itself is carried out locally by a user with authentication to the targeted system.

CVE-2023-23376 - Windows Common Log File System Driver Elevation of Privilege Vulnerability [4]

This vulnerability, with a CVSS score of 7.8, affects Windows Common Log File System Driver. An attacker who successfully exploited this vulnerability could gain SYSTEM privileges.

Affected Products

Global list of affected products by all the vulnerabilities are listed in the original advisory from Microsoft [1].

Recommendations

Microsoft and CERT-EU strongly recommend installing security updates as soon as possible.

References

[1] https://www.bleepingcomputer.com/news/microsoft/microsoft-february-2023-patch-tuesday-fixes-3-exploited-zero-days-77-flaws/

[2] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21823

[3] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21715

[4] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-23376

[5] https://www.bleepingcomputer.com/microsoft-patch-tuesday-reports/February-2023.html