MS-ISAC® Cybersecurity Advisory

TLP: CLEAR
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2023-030

DATE(S) ISSUED:
3/14/2023

SUBJECT:
Critical Patches Issued for Microsoft Products, March 14, 2023

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft products, the most severe of which could allow for remote code execution in the context of the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
Two zero-day vulnerabilities addressed in this advisory were reported by Microsoft; both have been seen in the wild. The first zero day, CVE-2023-23397 - Microsoft Outlook Elevation of Privilege Vulnerability, is a privilege elevation bug that allows specially crafted emails to force a target's device to connect to a remote URL and transmit the Windows account's Net-NTLMv2 hash, allowing an attacker to authenticate as the victim. The second zero day, CVE-2023-24880 - Windows SmartScreen Security Feature Bypass Vulnerability, allows an attacker to distribute and install malware by crafting a malicious file that would evade Mark of the Web (MOTW) defenses, resulting in a limited loss of integrity and availability of security features such as Protected View in Microsoft

Office, which rely on MOTW tagging.

SYSTEMS AFFECTED:

- Azure
- Client Server Run-time Subsystem (CSRSS)
- Internet Control Message Protocol (ICMP)
- Microsoft Bluetooth Driver
- Microsoft Dynamics
- Microsoft Edge (Chromium-based)
- Microsoft Graphics Component
- Microsoft Office Excel
- Microsoft Office Outlook
- Microsoft Office SharePoint
- Microsoft OneDrive
- Microsoft PostScript Printer Driver
- Microsoft Printer Drivers
- Microsoft Windows Codecs Library
- Office for Android
- Remote Access Service Point-to-Point Tunneling Protocol
- Role: DNS Server
- Role: Windows Hyper-V
- Service Fabric
- Visual Studio
- Windows Accounts Control
- Windows Bluetooth Service
- Windows Central Resource Manager
- Windows Cryptographic Services
- Windows Defender
- Windows HTTP Protocol Stack
- Windows HTTP.sys
- Windows Internet Key Exchange (IKE) Protocol
- Windows Kernel
- Windows Partition Management Driver
- Windows Point-to-Point Protocol over Ethernet (PPPoE)
- Windows Remote Procedure Call
- Windows Remote Procedure Call Runtime
- Windows Resilient File System (ReFS)
- Windows Secure Channel

- Windows SmartScreen
- Windows TPM
- Windows Win32K

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low
TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Microsoft products, the most severe of which could allow for remote code execution.

A full list of all vulnerabilities can be found at the link below:

https://learn.cisecurity.org/e/799323/update-guide/4ssjbj/846529329?h=baOnLPoR5tQSJWhRVklKk6jOgzTct1wcUO0i6Vb9HfI

Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged-on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
We recommend the following actions be taken:

- Apply appropriate patches or appropriate mitigations provided by Microsoft to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)
    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually,

or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
- Apply the Principle of Least Privilege to all systems and services, and run all software as a non-privileged user (one without administrative rights) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)
    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
    - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.
- Remind all users not to visit untrusted websites or follow links/open files provided by unknown or untrusted sources. (**M1017: User Training**)
    - **Safeguard 14.1: Establish and Maintain a Security Awareness Program:** Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks:** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.
- Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior. (**M1040 : Behavior Prevention on Endpoint**)
    - **Safeguard 13.2 : Deploy a Host-Based Intrusion Detection Solution**: Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.

Safeguard 13.7 : Deploy a Host-Based Intrusion Prevention Solution: Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

REFERENCES:

Microsoft:

https://msrc.microsoft.com/update-guide/
https://msrc.microsoft.com/update-guide/releaseNote/2023-Mar

Bleeping Computer:

https://learn.cisecurity.org/e/799323/ay-fixes-2-zero-days-83-flaws-/4ssjc7/846529329?h=baOnLPoR5tQSJWhRVklKk6jOgzTct1wcUO0i6Vb9HfI

Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061

24×7 Security Operations Center
SOC@cisecurity.org - 1-866-787-4722