Royal Ransomware Security Bulletin

DIR Cybersecurity Incident Response Team (CIRT)
Jan 10, 2023

SUBJECT: Critical Patches Issued for Microsoft Products, January 10, 2023

TLP: CLEAR

Announcement ID: 1165435
Date: 1/10/2023
Announcement Type: Actionable Intelligence
Importance: Standard
Distributed to: TX-ISAO: Everyone

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, one of which is currently being exploited in the wild. The first zero day is CVE-2023-21674 - Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability which is a Sandbox escape vulnerability that can lead to the elevation of privileges, and is currently being exploited in the wild. The second zero day is CVE-2023-21549 - Windows SMB Witness Service Elevation of Privilege Vulnerability and if exploited the attacker could execute RPC functions that are restricted to privileged accounts only.

SYSTEMS AFFECTED:

- NET Core
- 3D Builder
- Azure Service Fabric Container
- Microsoft Bluetooth Driver
- Microsoft Exchange Server

- Microsoft Graphics Component
- Microsoft Local Security Authority Server (lsasrv)
- Microsoft Message Queuing
- Microsoft Office
- Microsoft Office SharePoint
- Microsoft Office Visio
- Microsoft WDAC OLE DB provider for SQL
- Visual Studio Code
- Windows ALPC
- Windows Ancillary Function Driver for WinSock
- Windows Authentication Methods
- Windows Backup Engine
- Windows Bind Filter Driver
- Windows BitLocker
- Windows Boot Manager
- Windows Credential Manager
- Windows Cryptographic Services
- Windows DWM Core Library
- Windows Error Reporting
- Windows Event Tracing
- Windows IKE Extension
- Windows Installer
- Windows Internet Key Exchange (IKE) Protocol
- Windows iSCSI
- Windows Kernel
- Windows Layer 2 Tunneling Protocol
- Windows LDAP - Lightweight Directory Access Protocol
- Windows Local Security Authority (LSA)
- Windows Local Session Manager (LSM)
- Windows Malicious Software Removal Tool
- Windows Management Instrumentation
- Windows MSCryptDImportKey
- Windows NTLM
- Windows ODBC Driver

- Windows Overlay Filter
- Windows Point-to-Point Tunneling Protocol
- Windows Print Spooler Components
- Windows Remote Access Service L2TP Driver
- Windows RPC API
- Windows Secure Socket Tunneling Protocol (SSTP)
- Windows Smart Card
- Windows Task Scheduler
- Windows Virtual Registry Provider
- Windows Workstation Service

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/4r23t2/691143922?h=KU4ivtqvR4YphtYLwaPrvwTjy7rXzymr6JrA6Oy5-dA

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.

TLP:CLEAR = Recipients can spread this to the *world*, there is no limit on disclosure.

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-Jan

Supporting Documents:

TLP: CLEAR

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.

https://www.us-cert.gov/tlp

TLP:CLEAR = Recipients can spread this to the *world*, there is no limit on disclosure.

Assistance/Feedback/Questions?

Texas Information Sharing and Analysis Organization

DIRSecurity@dir.texas.gov

Submit a Threat Report

Texas ISAO Threat Reporting System

Sign up for News and Intelligence

TX-ISAO Mailing List Access Request Form

Texas Department of Information Resources

www.dir.texas.gov

Transforming How Texas Government Serves Texans