

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**TLP: WHITE**

[www.cisa.gov/tlp](http://www.cisa.gov/tlp)

**Information may be distributed without restriction, subject to standard copyright rules.**

**DATE(S) ISSUED:**

09/13/2022

**SUBJECT:**

Critical Patches Issued for Microsoft Products, September 13, 2022

**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:**

The zero-day privilege escalation vulnerability, CVE-2022-37969 (Windows Common Log File System Driver), has been reported by Microsoft as currently being exploited in the wild and has been fixed in this patch.

**SYSTEMS AFFECTED:**

- .NET and Visual Studio
- .NET Framework
- Azure Arc
- Cache Speculation
- HTTP.sys
- Microsoft Dynamics
- Microsoft Edge (Chromium-based)
- Microsoft Graphics Component
- Microsoft Office
- Microsoft Office SharePoint
- Microsoft Office Visio
- Microsoft Windows ALPC
- Microsoft Windows Codecs Library
- Network Device Enrollment Service (NDES)

- Role: DNS Server
- Role: Windows Fax Service
- SPNEGO Extended Negotiation
- Visual Studio Code
- Windows Common Log File System Driver
- Windows Credential Roaming Service
- Windows Defender
- Windows Distributed File System (DFS)
- Windows DPAPI (Data Protection Application Programming Interface)
- Windows Enterprise App Management
- Windows Event Tracing
- Windows Group Policy
- Windows IKE Extension
- Windows Kerberos
- Windows Kernel
- Windows LDAP - Lightweight Directory Access Protocol
- Windows ODBC Driver
- Windows OLE
- Windows Photo Import API
- Windows Print Spooler Components
- Windows Remote Access Connection Manager
- Windows Remote Procedure Call
- Windows TCP/IP
- Windows Transport Security Layer (TLS)

#### **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/3kbf2c/460565347?h=cPX31L9ywmlY7lavlYFrkuoYZULR10fCRc67D\\_mzyq4](https://learn.cisecurity.org/e/799323/update-guide/3kbf2c/460565347?h=cPX31L9ywmlY7lavlYFrkuoYZULR10fCRc67D_mzyq4)

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/2022-Sep>