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

DATE(S) ISSUED:
05/31/2022

SUBJECT:
A Vulnerability in Microsoft Support Diagnostic Tool (MSDT) Could Allow for Arbitrary Code Execution

OVERVIEW:
A vulnerability in Microsoft Support Diagnostic Tool (MSDT) could allow for arbitrary code execution. MSDT collects information from hosts running Microsoft Windows and Windows Server to send to Microsoft Support. Successful exploitation of this vulnerability could result in arbitrary code execution. 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:
CVE-2022-30190 (Follina) has been publicly disclosed and exploited in the wild. Attackers are executing arbitrary code via user execution of malicious word documents.

SYSTEMS AFFECTED:

- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2012
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 (Server Core installation)
- Windows Server 2016

- Windows Server 2016 (Server Core installation)
- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows Server, version 20H2 (Server Core Installation)
- Windows Server 2022 Azure Edition Core Hotpatch
- Windows Server 2022 (Server Core installation)
- Windows Server 2022
- Windows 7 for x64-based Systems Service Pack 1
- Windows 7 for 32-bit Systems Service Pack 1
- Windows RT 8.1
- Windows 8.1 for x64-based systems
- Windows 8.1 for 32-bit systems
- Windows 10 for x64-based Systems
- Windows 10 for 32-bit Systems
- Windows 10 Version 1607 for x64-based Systems
- Windows 10 Version 1607 for 32-bit Systems
- Windows 10 Version 1809 for ARM64-based Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows 10 Version 1809 for 32-bit Systems
- Windows 10 Version 20H2 for ARM64-based Systems
- Windows 10 Version 20H2 for 32-bit Systems
- Windows 10 Version 20H2 for x64-based Systems
- Windows 10 Version 21H1 for 32-bit Systems
- Windows 10 Version 21H1 for ARM64-based Systems
- Windows 10 Version 21H1 for x64-based Systems
- Windows 10 Version 21H2 for x64-based Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 21H2 for 32-bit Systems
- Windows 11 for ARM64-based Systems
- Windows 11 for x64-based Systems

RISK:

Government:

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

Businesses:

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

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in Microsoft Support Diagnostic Tool (MSDT) which could allow for arbitrary code execution. MSDT can be called using the URL protocol from a calling application like Word allowing an attacker to run arbitrary code with the privileges of the user that executed the program. An attacker can entice a victim to open a malicious Word document resulting in code execution without macros enabled. The attacker can then install programs, view, change, or delete data, or create new accounts in the context allowed by the user's rights. Following the MITRE ATT&CK framework, exploitation of this vulnerability can be classified as follows:

Tactic: *Execution* **(**TA0002**)**:

Technique: *User Execution* **(**T1204**):**

- An arbitrary code execution vulnerability (CVE-2022-30190)

Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code 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.

RECOMMENDATIONS:
We recommend the following actions be taken:

- There is currently not a patch available for this vulnerability. **All admins should apply the workaround released by Microsoft, which disables MSDT URL protocol thus preventing exploitation**. (See the second link under the Microsoft references below.) **NOTE:** After Microsoft releases a CVE-2022-30190 patch, you can undo the workaround by launching an elevated command prompt and executing the reg import filename command (filename is the name of the registry backup created when disabling the protocol). (**M1051: Update Software, M1042: Disable or Remove Feature or Program**)
    - **Safeguard 4.8: Uninstall or Disable Unnecessary Services on Enterprise Assets and Software:** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.
    - **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. Run all software as a non-privileged user (one without administrative privileges) 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.
- 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/vulnerability/CVE-2022-30190
https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30190

PCmag:
https://www.pcmag.com/news/researchers-reveal-follina-zero-day-vulnerability-in-microsoft-office