Guidance for CVE-2022-30190 Microsoft Support Diagnostic Tool Vulnerability

MSRC / By MSRC / May 30, 2022 / 4 min read

UPDATE July 12, 2022: As part of the response by Microsoft, a defense in depth variant has been found and fixed in the Windows July cumulative updates. Microsoft recommends installing the July updates as soon as possible.

Windows Version	Link to KB article	LInk to Catalog
Windows 8.1, Windows Server 2012 R2	5015805	Download
Windows Server 2012	5015805	Download
Windows 7, Windows Server 2008 R2	5015805	Download
Windows Server 2008 SP2	5015805	Download

On Monday May 30, 2022, Microsoft issued CVE-2022-30190 regarding the Microsoft Support Diagnostic Tool (MSDT) in Windows vulnerability. On Tuesday June 14, 2022, Microsoft issued Windows updates to address this vulnerability. Microsoft recommends installing the following KB5015805 for Windows 8.1 and below according to the following table. The defense in depth fix is incorporated into the cumulative updates for Windows 10 and newer.

A remote code execution vulnerability exists when MSDT is called using the URL protocol from a calling application such as Word. An attacker who successfully exploits this vulnerability can run arbitrary code with the privileges of the calling application. The attacker can then install programs, view, change, or delete data, or create new accounts in the context allowed by the user's rights.

Workarounds

To disable the MSDT URL Protocol

Disabling MSDT URL protocol prevents troubleshooters being launched as links including links throughout the operating system. Troubleshooters can still be accessed using the Get Help application and in system settings as other or additional troubleshooters. Follow these steps to disable:

1. Run **Command Prompt** as **Administrator**.
2. To back up the registry key, execute the command "reg export HKEY*CLASSES_ROOT\ms-msdt _filename*"
3. Execute the command "reg delete HKEY_CLASSES_ROOT\ms-msdt /f".

How to undo the workaround

1. Run **Command Prompt** as **Administrator**.
2. To restore the registry key, execute the command "reg import *filename*"

Microsoft Defender Detections & Protections

Microsoft Defender Antivirus (MDAV)

Microsoft Defender Antivirus provides detections and protections for possible vulnerability exploitation under the following signatures using detection build **1.367.851.0** or higher:

Search blog posts

Subscribe

Categories

MSRC (1077)
Japan Security Team (1041)
Security Research & Defense (384)
BlueHat (192)
Bug Bounty Programs (11)
Microsoft Threat Hunting (5)

Tags

セキュリティ情報 (465)
脆弱性 (248)
アドバイザリ (183)
Internet Explorer (IE) (156)
Security Update (140)
Security Advisory (135)
Security Bulletin (133)
Mitigations (128)
Community-based Defense (114)
セキュリティ更新 (113)
View all Tags

Recent Posts

Congratulations to the Top MSRC 2024 Q3 Security Researchers!
Announcing the BlueHat 2024 Sessions
Announcing BlueHat 2024: Call for Papers now open
Congratulations to the MSRC 2024 Most Valuable Security Researchers!
Microsoft Bounty Program Year in Review: $16.6M in Rewards

Archives

October 2024 (3)
September 2024 (1)
August 2024 (5)

- **Trojan:Win32/Mesdetty.A**
- **Trojan:Win32/Mesdetty.B**
- **Behavior:Win32/MesdettyLaunch.A!blk**
- **Trojan:Win32/MesdettyScript.A**
- **Trojan:Win32/MesdettyScript.B**
- **Behavior:Win32/MesdettyPayload.B**
- **Behavior:Win32/MesdettyLaunch.D**

July 2024 (8)

June 2024 (6)

View full Archive

Customers with Microsoft Defender Antivirus (MDAV) should turn-on cloud-delivered protection and automatic sample submission. These capabilities use artificial intelligence and machine learning to quickly identify and stop new and unknown threats.

Microsoft Defender for Endpoint (MDE)

Microsoft Defender for Endpoint provides customers detections and alerts. The following alert title in the Microsoft 365 Defender portal can indicate threat activity on your network:

- **Suspicious behavior by an Office application**
- **Suspicious behavior by Msdt.exe**

Microsoft Defender for Endpoint through its network inspection capabilities created a network-based detection to intercept any possible exploits for this vulnerability over the internal network.

- **Possible exploitation attempt of CVE-2022-30190**

and since the signatures above for Antivirus are getting expanded to include more scenarios I like to remove the sentences between brackets for each signature

- **Trojan:Win32/Mesdetty.A** (blocks msdt command line)
- **Trojan:Win32/Mesdetty.B** (blocks msdt command line)
- **Behavior:Win32/MesdettyLaunch.A!blk** (terminates the process that launched msdt command line)
- **Trojan:Win32/MesdettyScript.A** (to detect HTML files that contain msdt suspicious command being dropped)
- **Trojan:Win32/MesdettyScript.B** (to detect HTML files that contain msdt suspicious command being dropped)

Microsoft Defender for Office 365 (MDO)

Microsoft Defender for Office 365 provides detections and protection for emails containing malicious documents or URL used to exploit this vulnerability:

- Trojan_DOCX_OLEAnomaly_AC
- Trojan_DOCX_OLEAnomaly_AD
- Trojan_DOCX_OLEAnomaly_AE
- Trojan_DOCX_OLEAnomaly_AF
- Exploit_UIA_CVE_2022_30190
- Exploit_CVE_2022_30190_ShellExec
- Exploit_HTML_CVE_2022_30190_A
- Exploit_Win32_CVE_2022_30190_B

FAQ

Q: Does Protected View and Application Guard for Office provide protection from this vulnerability?

A: If the calling application is a Microsoft Office application, by default, Microsoft Office opens documents from the internet in Protected View or Application Guard for Office, both of which prevent the current attack.

- For information about Protected View, see What is Protected View?
- For information about Application Guard for Office, see Application Guard for Office.

Q: Is configuring the GPO setting **Computer Configuration\Administrative Templates\System\Troubleshooting and Diagnostics\Microsoft Support Diagnostic Tool\"Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider"** to **"Disabled"** another workaround?

```
Registry Hive: HKEY_LOCAL_MACHINE Registry Path:
\Software\Policies\Microsoft\Windows\ScriptedDiagnosticsProvider\Policy\ Value Name:
DisableQueryRemoteServer Type: REG_DWORD Value: 0
```

A: No, this GPO does not provide protection against this vulnerability. “Interactive communication with support provider” is a special mode MSDT runs in when launched with no parameters which has no impact on MSDT support for URL protocol.

Q: Is configuring the GPO setting **Computer Configuration - Administrative Templates - System - Troubleshooting and Diagnostics - Microsoft Support Diagnostic Tool\“Troubleshooting: Allow users to access recommended troubleshooting for known problems”** to " **Disabled**" another workaround?

A: No, enabling or disabling this group policy has no effect on the vulnerable part of Troubleshooter functionality, so it is not a viable workaround.

Q: Is blocking MSDT using technologies such as Windows Defender Application Control (WDAC) equivalent to removing MSDT handler “HKEY_CLASSES_ROOT\ms-msdt” a viable workaround?

A: Blocking MSDT will prevent all MSDT-based Windows Troubleshooters from launching, such as the Network Troubleshooter, and the Printer Troubleshooter. The recommended workaround disables support for clicking on MSDT links and users can continue to use the familiar Windows Troubleshooters.

Q : What Windows versions require the workaround?

A : The MSDT URL protocol is available in Windows Server 2019 & Windows 10 version 1809 and later supported versions of Windows. The registry key mentioned in the workaround section will not exist in earlier supported versions of Windows, so the workaround is not required.

We will update CVE-2022-30190 with further information.

The MSRC Team

Revisions:
06/06/2022 - Added more FAQs.
06/07/2022 - Added one more question and answer.
06/07/2022 - Added additional detection information.
06/14/2022 - Announced updates that address the vulnerability.
07/12/2022 - Announced defense in depth update availability.

Previous Post Next Post