NCSC
National Cyber Security Centre

2206151000-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Attackers Exploiting MSProtocol URI scheme UPDATE 2

CVE-2022-30190

2022-06-15

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

Revision History

Revision	Date	Author(s)	Description
1.0	30 May 2022	CSIRT-IE	Initial Alert created regarding actively exploited zero day affecting Microsoft products
1.1	31 May 2022	CSIRT-IE	Alert updated to include details of Microsofts' workaround and published CVE number for this vulnerability
1.2	07 June 2022	CSIRT-IE	Changes made to affected products
1.3	15 June 2022	CSIRT-IE	Microsoft release patch for vulnerability

Description

On 27th May 2022, Japanese cyber security research team *Nao_Sec* observed on Virus Total a recently discovered exploitation of Microsofts' Support Diagnostics Tool - **"ms-msdt"** to execute PowerShell code in Microsoft Office documents. **"ms-msdt"** is used in Microsoft products to invoke a troubleshooting pack at the command line or as part of an automated script, and enables additional options without user input.

This method allows attackers to use Microsoft Products to execute code via msdt even if macros are disabled. Protected View will stop execution of this vulnerability in some cases, however conversion of documents to RTF files will allow the exploit to run without even opening the document (in preview mode).

On Monday 30 May 2022, Microsoft issued CVE-2022-30190 regarding the Microsoft Support Diagnostic Tool (MSDT) in Windows vulnerability. Attackers have been observed using this method in the wild, the NCSC expects to see continued exploitation of this vulnerability by threat actors against unpatched systems.

More information regarding this vulnerability can be found at the following link: MSRC Security Updates and at Microsofts Blog: Guidance for CVE-2022-30190 Microsoft Support Diagnostic Tool Vulnerability

Products Affected

Mutliple versions of Microsoft Operating systems are affected by this vulnerability, including versions of:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012
- Windows Server 2008
- Windows 11
- Windows 10
- Windows 8.1
- Windows 7

The full list of affected products can be found at https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190

Impact

Remote Code Execution (RCE)
Arbitrary Code Execution

Recommendations

An update patching this vulnerability is included in the June 2022 cumulative Windows Updates. The NCSC recommends that organisations install the updates as a matter of priority. Organisations whose systems are configured to receive automatic updates are not required to manually install the update.

Organisations should also monitor their systems for suspicious behaviour related to these types of attacks. A number of security reserachers have released various monitoring and detection rules including:

- Microsoft Sentinel Query
- Huntress msdt Execution Sigma Rule
- SigmaHQ:master, Sigma Rule

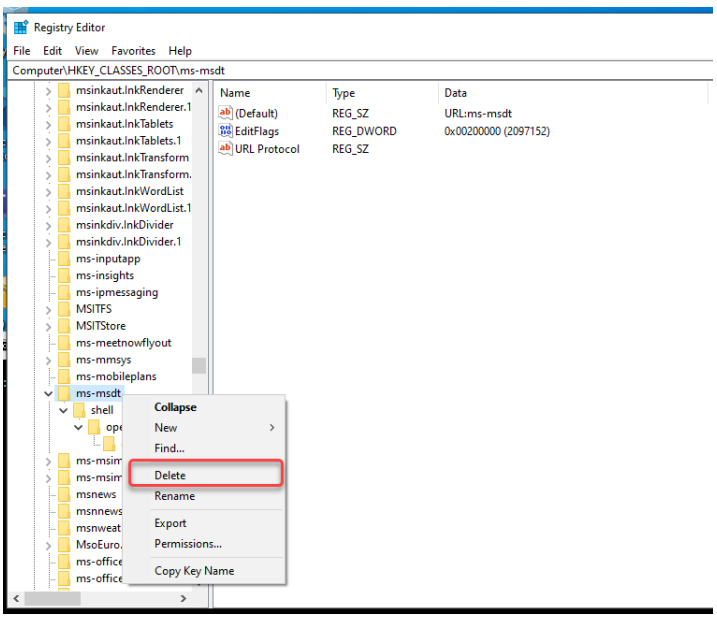
Organisations unable to immediately apply the update should consider the potential workaround for this issue and backup and delete their msdt registry key. This will affect the legitimate functionality of the msdt function so please be aware of the adverse affects of applying this workaround:

Workaround:

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 back up the registry key, execute the command “reg import *filename*”



DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie