NOTIFIKASI KERENTANAN *MICROSOFT SUPPORT DIAGNOSTIC TOOL (MSDT)* PADA CVE 2022-30190

RINGKASAN EKSEKUTIF

1. CVE-2022-30190 memiliki nilai **7,8** dengan tingkat dampak **HIGH**. Kerentanan ini terdapat pada layanan Microsoft Support Diagnostic Tool (MSDT) yang merupakan salah satu produk dari Microsoft Corporation.
2. Penyebab utama kerentanan ini berkaitan dengan adanya kelemahan ketika MSDT diakses menggunakan protokol URL dari *calling application* seperti Word.
3. Langkah yang dapat dilakukan untuk terhindar dari kerentanan ini adalah dengan menonaktifkan protokol URL MSDT dan melakukan *patching* sesuai dengan *security updates* yang dikeluarkan oleh Microsoft pada 14 Juni 2022.

NOTIFIKASI KERENTANAN

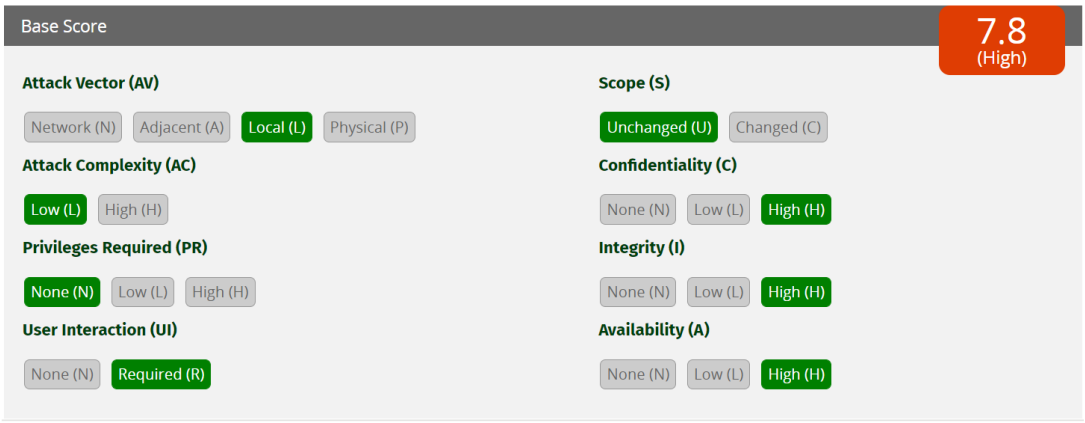
1. Microsoft Support Diagnostic Tool (MSDT) merupakan sebuah produk perangkat lunak yang dikembangkan oleh Microsoft Corporation dan berfungsi untuk menganalisis data diagnostik dan menemukan solusi untuk masalah perangkat pengguna. Produk ini terdapat pada Windows 11, Windows 10, Windows 8.1, Windows 7, dan Windows Server.
2. Produk yang memiliki kerentanan CVE-2022-30190 adalah semua versi Microsoft Office, mulai dari 2013 hingga yang terbaru, pada semua sistem operasi Windows yang menyediakan layanan MSDT. Berikut daftar produk yang tedampak kerentanan CVE-2022-30190:

Tabel 1. Daftar Produk Terdampak CVE-2022-30190

No	Nama Produk	No	Nama Produk
1.	Windows Server 2022 (Server Core Installation)	19.	Windows 10 Version 21H1 for x64-based Systems
2.	Windows Server 2022	20.	Windows 10 Version 21H1 for x64-based Systems
3.	Windows Server 2, version 20H2 (Server Core Installation)	21.	Windows 10 Version 21H1 for ARM64-based Systems
4.	Windows Server 2019 (Server Core Installation)	22.	Windows 10 Version 21H1 for 32-bit Systems
5.	Windows Server 2019	23.	Windows 10 Version 20H2 for x64-based Systems

6.	Windows Server 2016 (Server Core Installation)	24.	Windows 10 Version 20H2 for ARM64-based Systems
7.	Windows Server 2016	25.	Windows 10 Version 20H2 for 32-bit Systems
8.	Windows Server 2012 R2 (Server Core Installation)	26.	Windows 10 Version 1809 for x64-based Systems
9.	Windows Server 2012 R2	27.	Windows 10 Version 1809 for ARM64-based Systems
10.	Windows Server 2012 (Server Core Installation)	28.	Windows 10 Version 1809 for 32-bit Systems
11.	Windows Server 2012	29.	Windows 10 Version 1607 for x64-based Systems
12.	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core Installation)	30.	Windows 10 for x64-based Systems
13.	Windows Server 2008 R2 for x64-based Systems Service Pack 1	31.	Windows 10 for 32-bit Systems
14.	Windows 11 for x64-based Systems	32.	Windows RT 8.1
15.	Windows 11 for ARM64-based Systems	33.	Windows 8.1 for x64-based Systems
16.	Windows 10 Version 21H2 for x64-based Systems	34.	Windows 8.1 for 32-bit Systems
17.	Windows 10 Version 21H2 for ARM64-based Systems	35.	Windows 7 for x64-based Systems Service Pack 1
18.	Windows 10 Version 21H2 for 32-bit Systems	36.	Windows 7 for 32-bit Systems Service Pack 1

3. CVE-2022-30190 yang dijuluki dengan kode kota Italia, Follina, merupakan serangan *Remote Code Execution* (RCE) yang terjadi karena kelemahan pada saat MSDT diakses menggunakan protokol URL dari *calling application* seperti Word. Berikut adalah perhitungan dari kerentanan berdasarkan https://www.first.org/cvss/calculator:



Gambar 1. Perhitungan Nilai Kerentanan

Berdasarkan perhitungan tersebut, diperoleh informasi bahwa akses sistem secara lokal sebagai *Attack Vector* (AV). Hal tersebut disebabkan karena penyerang bergantung pada interaksi pengguna untuk melakukan tindakan yang diperlukan untuk mengeksploitasi kerentanan, yaitu pengguna membuka file berbahaya. Selain itu, Follina memiliki *Attack Complexity* (AC) yang rendah dan tidak memerlukan *privilege.* Namun, diperlukan *user interaction* dalam proses serangan. Apabila kerentanan ini berhasil dieksploitasi, maka akan memiliki nilai resiko yang tinggi terhadap aspek kerahasiaan, integritas, dan ketersediaan.

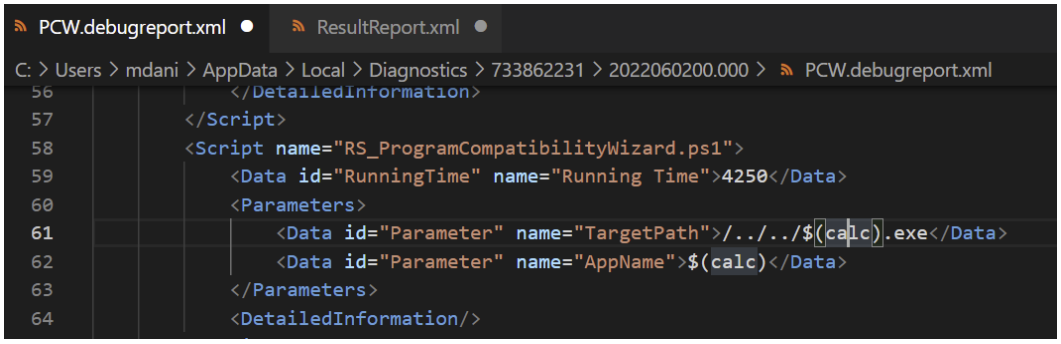
4. Berikut merupakan langkah-langkah atau prosedur dari kerentanan CVE-2022-30190:
   a. Penyerang mengirim *e-mail* yang berisi dokumen Microsoft Office berbahaya (.docx, dll.) ke pengguna yang ditargetkan.
   b. Pengguna mengeksekusi file tersebut yang dapat menyelesaikan dan mengeksekusi sumber daya eksternal yang dikendalikan penyerang dari file document.xml.ref.
   c. Kode yang mengeksploitasi kerentanan Follina dijalankan kepada pengguna.
   d. Kode ini kemudian meluncurkan perintah tambahan seperti mengunduh *Remote Access Trojan*, dan lain sebagainya.
5. Dampak dari kerentanan ini adalah penyerang dapat menjalankan perintah dengan izin aplikasi yang digunakan untuk membuka dokumen berbahaya. Menurut Microsoft, penyerang juga dapat menginstal program, melihat, mengubah, menghapus data, atau membuat akun baru. Penyerang yang berhasil mengeksploitasi kerentanan ini dapat menjalankan kode arbitrer dengan hak istimewa *calling application*.
6. Terdapat cara-cara yang digunakan untuk dapat melakukan deteksi terkait sistem terdampak melalui "`/dt`" *command line parameter*:

   a. `%LOCALAPPDATA%\Diagnostics`
   b. `%LOCALAPPDATA%\ElevatedDiagnostics`

   Pada sistem pengujian Qualys Research Team's, data diagnostik disimpan di dalam:

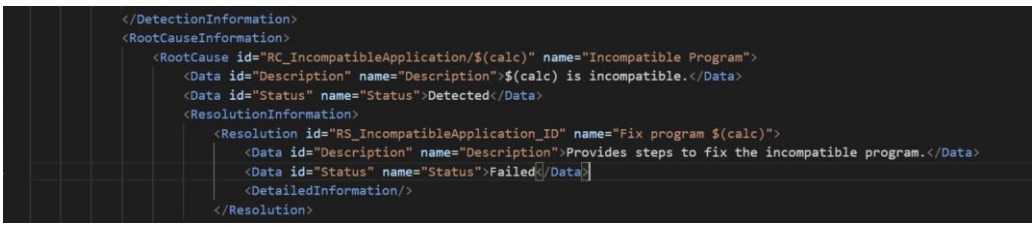
   `%LOCALAPPDATA%\Diagnostics\<9-digit-number>\<tanggal YYYYMMDD.000>`

Direktori ini berisi beberapa file yang dapat membantu personel *Digital Forensics* dan *Incident Response* untuk menentukan file apa yang dijalankan. Misalnya, Gambar 2 adalah kutipan dari file `PCW.debugreport.xml` di salah satu sistem pengujian yang menunjukkan jalur dan biner yang dijalankan:



Gambar 2. Nilai AppName di PCW.debugreport.xml yang Menggambarkan Perintah yang Dijalankan Melalui Follina

Selain itu, jika file XML di atas dirusak, file ResultReport.xml juga memberi kita lebih banyak detail seperti yang ditunjukkan di bawah ini (Gambar 3):



Gambar 3. Informasi Forensik Tambahan Ada di ResultReport.xml

REKOMENDASI

1. Menonaktifkan protokol URL MSDT dengan cara sebagai berikut:
   a. Jalankan Command Prompt sebagai Administrator.
   b. Untuk melakukan *back up registry key,* jalankan perintah "`reg export HKEY_CLASSES_ROOT\ms-msdt filename`".
   c. Kemudian jalankan perintah "`reg delete HKEY_CLASSES_ROOT\ms-msdt /f`".

   Apabila ingin mengembalikan pengaturan seperti semula, dapat dilakukan dengan cara sebagai berikut:
   a. Jalankan Command Prompt sebagai Administrator.

b. Untuk melakukan *restore registry key* dapat dilakukan dengan menjalankan perintah "`reg import filename`" yang menunjuk ke file cadangan yang dibuat sebelum menonaktifkan MSDT.

2. Selain solusi melalui MSDT, dapat juga dilakukan perbaikan untuk eksploitasi melalui “search-mas” dengan menonaktifkan protokol URL “ms-search” sebagai berikut:
   a. Jalankan Command Prompt sebagai Administrator.
   b. Untuk melakukan *back up registry key,* jalankan perintah "`reg export HKEY_CLASSES_ROOT\search-ms filename`".
   c. Jalankan perintah “`reg delete HKEY_CLASSES_ROOT\search-ms /f`”.

   Apabila ingin mengembalikan pengaturan seperti semula, dapat dilakukan dengan cara sebagai berikut:
   a. Jalankan Command Prompt sebagai Administrator.
   b. Untuk melakukan *restore registry key,* jalankan perintah "`reg import filename`" yang menunjuk ke file cadangan yang telah dibuat di bagian sebelumnya.
3. Memberikan literasi kepada publik maupun stakeholder terkait mitigasi terhadap kerentanan CVE-2022-30190.
4. Melakukan perlindungan dengan menggunakan Microsoft Defender Antivirus (MDAV) yang mampu mendeteksi dan melindungi eksploitasi kerentanan dengan deteksi build 1.367.851.0 atau yang lebih tinggi. Selain itu, dapat juga digunakan Microsoft Defender for Endpoint untuk deteksi dan perlindungan pada aplikasi Office dan Msdt.exe.
5. Untuk mencegah kerentanan CVE-2022-30190, lakukan pemeriksaan hubungan parent-child, yaitu proses msdt.exe yang dimulai oleh proses induk seperti word.exe atau excel.exe. Selain itu, perlu untuk mencegah Office membuat child process dengan membuat ASL rule: `Set-MpPreference -AttackSurfaceReductionRules_Ids d4f940ab-401b-4efc-aadc-ad5f3c50688a -AttackSurfaceReductionRules_Actions Enabled`