SECURE_CODING_LAB_13

NAME:M.KARTHIK

REG_N:19BCN7222

ASSIGNMENT-13

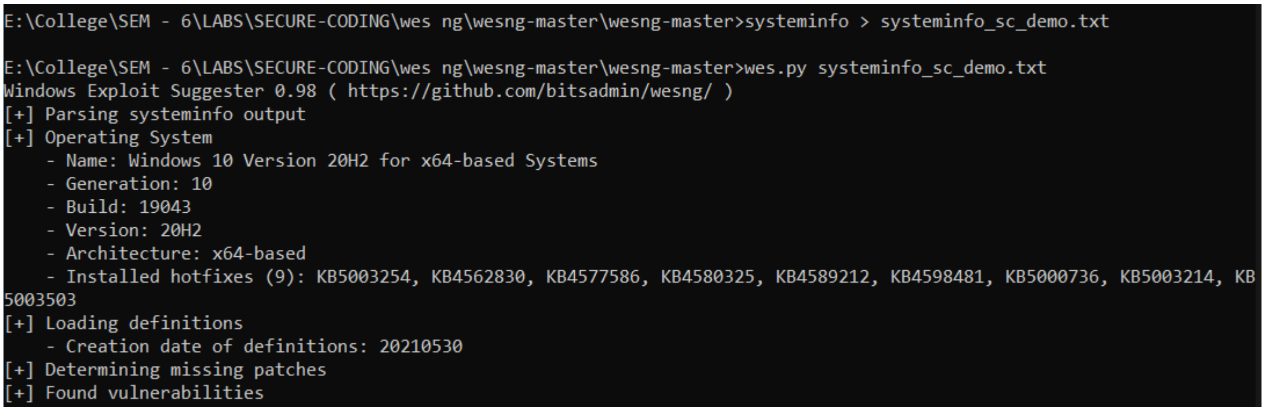
Windows exploit suggester:

This is a tool that helps you to identify the vulnerability in your naïve windows system.

Follow the link in github to download the files required….. https://github.com/bitsadmin/wesng

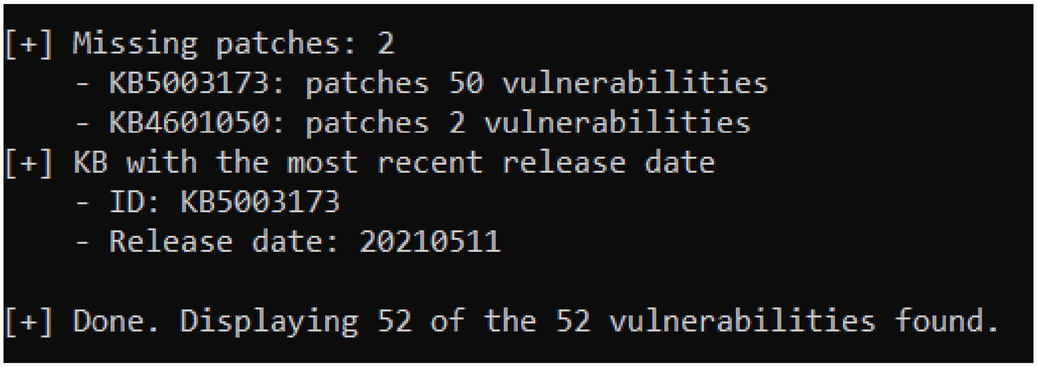
Double click on the **setup.py** to setup windows exploit

suggester. Now open command prompt do as follows



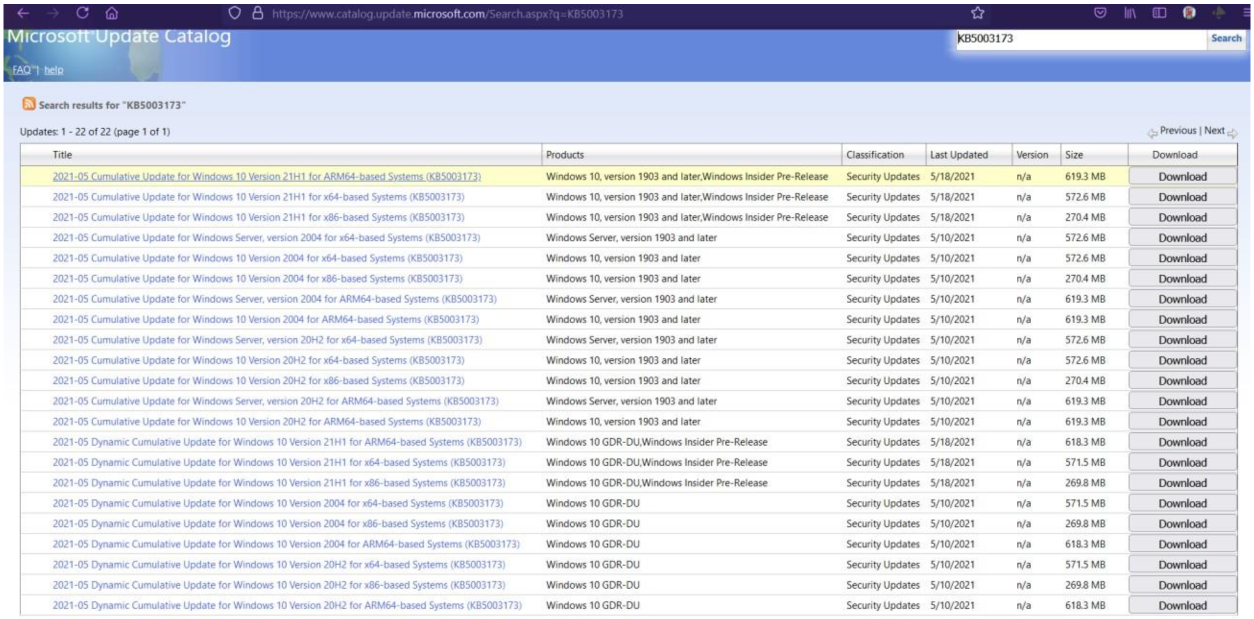
```
E:\College\SEM - 6\LABS\SECURE-CODING\wes ng\wesng-master\wesng-master>systeminfo > systeminfo_sc_demo.txt

E:\College\SEM - 6\LABS\SECURE-CODING\wes ng\wesng-master\wesng-master>wes.py systeminfo_sc_demo.txt
Windows Exploit Suggester 0.98 ( https://github.com/bitsadmin/wesng/ )
[+] Parsing systeminfo output
[+] Operating System
    - Name: Windows 10 Version 20H2 for x64-based Systems
    - Generation: 10
    - Build: 19043
    - Version: 20H2
    - Architecture: x64-based
    - Installed hotfixes (9): KB5003254, KB4562830, KB4577586, KB4580325, KB4589212, KB4598481, KB5000736, KB5003214, KB
5003503
[+] Loading definitions
    - Creation date of definitions: 20210530
[+] Determining missing patches
[+] Found vulnerabilities
```

Pipe the systeminfo as a txt file to the wes.py and it will list all the vulnerabilities in the system. At last it will give you all the patches that are required to patch the vulnerabilities as below.



```
[+] Missing patches: 2
    - KB5003173: patches 50 vulnerabilities
    - KB4601050: patches 2 vulnerabilities
[+] KB with the most recent release date
    - ID: KB5003173
    - Release date: 20210511

[+] Done. Displaying 52 of the 52 vulnerabilities found.
```

Now go to the Microsoft catalog to download the required hotfixes I will be like below.

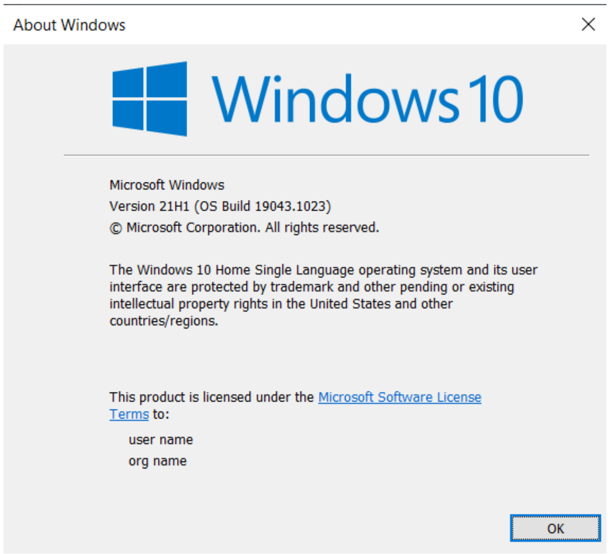

https://www.catalog.update.microsoft.com/Search.aspx?q=KB5003173
Microsoft Update Catalog
KB5003173
Search
FAQ | help
Previous | Next

Search results for "KB5003173"

Updates: 1 - 22 of 22 (page 1 of 1)

Title	Products	Classification	Last Updated	Version	Size	Download
2021-05 Cumulative Update for Windows 10 Version 21H1 for ARM64-based Systems (KB5003173)	Windows 10, version 1903 and later,Windows Insider Pre-Release	Security Updates	5/18/2021	n/a	619.3 MB	Download
2021-05 Cumulative Update for Windows 10 Version 21H1 for x64-based Systems (KB5003173)	Windows 10, version 1903 and later,Windows Insider Pre-Release	Security Updates	5/18/2021	n/a	572.6 MB	Download
2021-05 Cumulative Update for Windows 10 Version 21H1 for x86-based Systems (KB5003173)	Windows 10, version 1903 and later,Windows Insider Pre-Release	Security Updates	5/18/2021	n/a	270.4 MB	Download
2021-05 Cumulative Update for Windows Server, version 2004 for x64-based Systems (KB5003173)	Windows Server, version 1903 and later	Security Updates	5/10/2021	n/a	572.6 MB	Download
2021-05 Cumulative Update for Windows 10 Version 2004 for x64-based Systems (KB5003173)	Windows 10, version 1903 and later	Security Updates	5/10/2021	n/a	572.6 MB	Download
2021-05 Cumulative Update for Windows 10 Version 2004 for x86-based Systems (KB5003173)	Windows 10, version 1903 and later	Security Updates	5/10/2021	n/a	270.4 MB	Download
2021-05 Cumulative Update for Windows Server, version 2004 for ARM64-based Systems (KB5003173)	Windows Server, version 1903 and later	Security Updates	5/10/2021	n/a	619.3 MB	Download
2021-05 Cumulative Update for Windows 10 Version 2004 for ARM64-based Systems (KB5003173)	Windows 10, version 1903 and later	Security Updates	5/10/2021	n/a	619.3 MB	Download
2021-05 Cumulative Update for Windows Server, version 20H2 for x64-based Systems (KB5003173)	Windows Server, version 1903 and later	Security Updates	5/10/2021	n/a	572.6 MB	Download
2021-05 Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB5003173)	Windows 10, version 1903 and later	Security Updates	5/10/2021	n/a	572.6 MB	Download
2021-05 Cumulative Update for Windows 10 Version 20H2 for x86-based Systems (KB5003173)	Windows 10, version 1903 and later	Security Updates	5/10/2021	n/a	270.4 MB	Download
2021-05 Cumulative Update for Windows Server, version 20H2 for ARM64-based Systems (KB5003173)	Windows Server, version 1903 and later	Security Updates	5/10/2021	n/a	619.3 MB	Download
2021-05 Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows 10, version 1903 and later	Security Updates	5/10/2021	n/a	619.3 MB	Download
2021-05 Dynamic Cumulative Update for Windows 10 Version 21H1 for ARM64-based Systems (KB5003173)	Windows 10 GDR-DU,Windows Insider Pre-Release	Security Updates	5/18/2021	n/a	618.3 MB	Download
2021-05 Dynamic Cumulative Update for Windows 10 Version 21H1 for x64-based Systems (KB5003173)	Windows 10 GDR-DU,Windows Insider Pre-Release	Security Updates	5/18/2021	n/a	571.5 MB	Download
2021-05 Dynamic Cumulative Update for Windows 10 Version 21H1 for x86-based Systems (KB5003173)	Windows 10 GDR-DU,Windows Insider Pre-Release	Security Updates	5/18/2021	n/a	269.8 MB	Download
2021-05 Dynamic Cumulative Update for Windows 10 Version 2004 for x64-based Systems (KB5003173)	Windows 10 GDR-DU	Security Updates	5/10/2021	n/a	571.5 MB	Download
2021-05 Dynamic Cumulative Update for Windows 10 Version 2004 for x86-based Systems (KB5003173)	Windows 10 GDR-DU	Security Updates	5/10/2021	n/a	269.8 MB	Download
2021-05 Dynamic Cumulative Update for Windows 10 Version 2004 for ARM64-based Systems (KB5003173)	Windows 10 GDR-DU	Security Updates	5/10/2021	n/a	618.3 MB	Download
2021-05 Dynamic Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB5003173)	Windows 10 GDR-DU	Security Updates	5/10/2021	n/a	571.5 MB	Download
2021-05 Dynamic Cumulative Update for Windows 10 Version 20H2 for x86-based Systems (KB5003173)	Windows 10 GDR-DU	Security Updates	5/10/2021	n/a	269.8 MB	Download
2021-05 Dynamic Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows 10 GDR-DU	Security Updates	5/10/2021	n/a	618.3 MB	Download

Download the appropriate hotfixes for your pc type **winver** in start to get the version of the pc you are using. Download your hotfixes and fix your vulnerabilities.

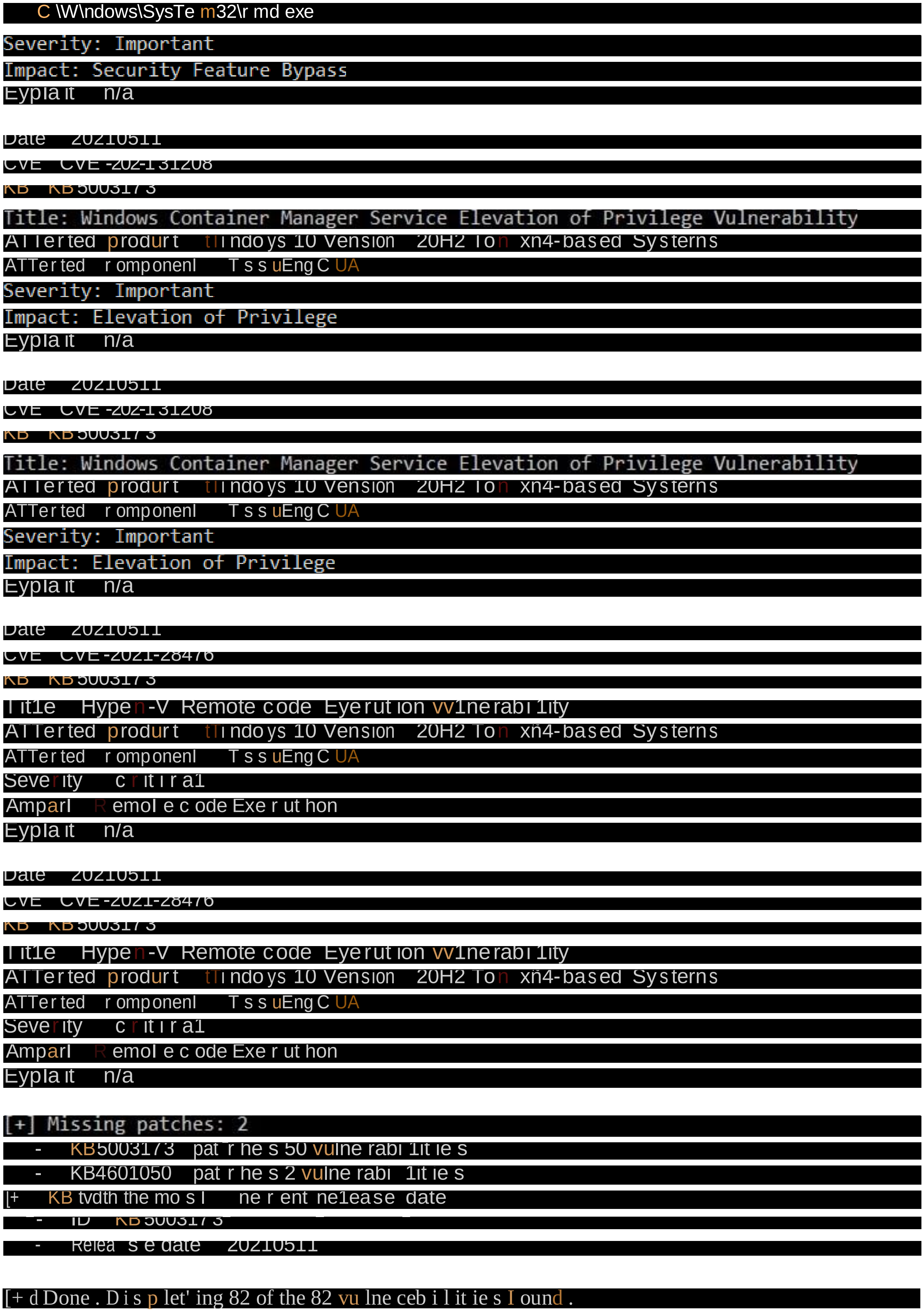


Microsoft Windows
Version 21H1 (OS Build 19043.1023)
© Microsoft Corporation. All rights reserved.

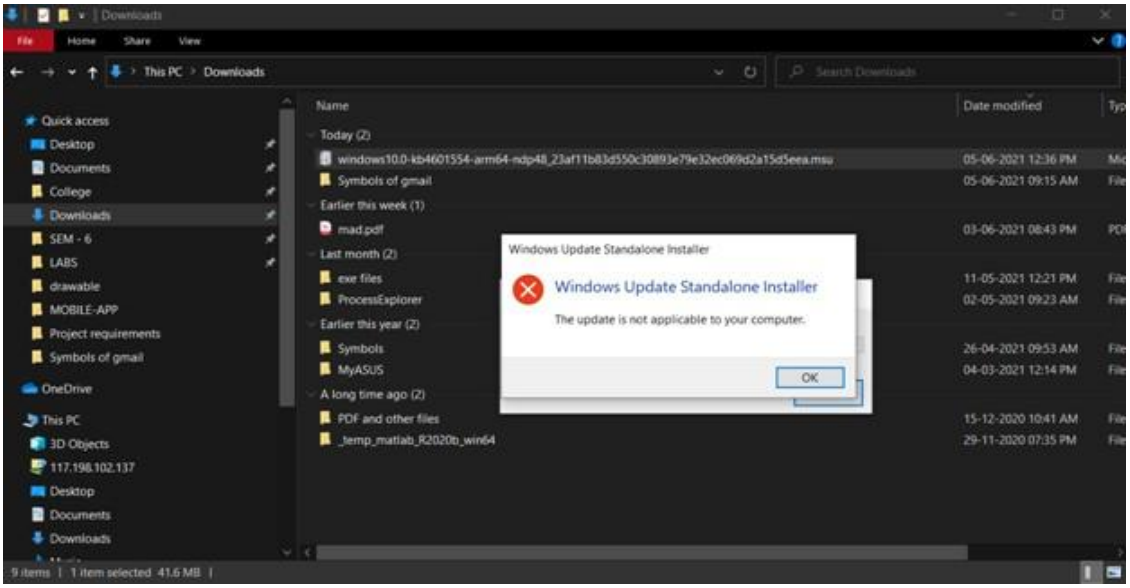
The Windows 10 Home Single Language operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.

This product is licensed under the Microsoft Software License Terms to:

user name
org name



```
    C \W\ndows\SysTe m32\r md exe
Severity: Important
Impact: Security Feature Bypass
Eypla it    n/a

Date   20210511
CVE   CVE -202-131208
KB   KB 500317 3
Title: Windows Container Manager Service Elevation of Privilege Vulnerability
ATTerted  produrt    tlindoys 10 Vension   20H2 Ton  xn4-based Systerns
ATTerted   r omponenl     T s s uEng C UA
Severity: Important
Impact: Elevation of Privilege
Eypla it    n/a

Date   20210511
CVE   CVE -202-131208
KB   KB 500317 3
Title: Windows Container Manager Service Elevation of Privilege Vulnerability
ATTerted  produrt    tlindoys 10 Vension   20H2 Ton  xn4-based Systerns
ATTerted   r omponenl     T s s uEng C UA
Severity: Important
Impact: Elevation of Privilege
Eypla it    n/a

Date   20210511
CVE   CVE -2021-28476
KB   KB 500317 3
T it1e    Hypen-V  Remote code  Eyerut ion vv1ne rabı 1ıty
ATTerted  produrt    tlindoys 10 Vension   20H2 Ton  xñ4-based Systerns
ATTerted   r omponenl     T s s uEng C UA
Sever ity     c r it i r a1
Amparl    R emol e c ode Exe r ut hon
Eypla it    n/a

Date   20210511
CVE   CVE -2021-28476
KB   KB 500317 3
T it1e    Hypen-V  Remote code  Eyerut ion vv1ne rabı 1ıty
ATTerted  produrt    tlindoys 10 Vension   20H2 Ton  xñ4-based Systerns
ATTerted   r omponenl     T s s uEng C UA
Sever ity     c r it i r a1
Amparl    R emol e c ode Exe r ut hon
Eypla it    n/a

[+] Missing patches: 2
     -    KB5003173   pat r he s 50 vulne rabı 1it ie s
     -    KB4601050   pat r he s 2 vulne rabı  1it ie s
[+    KB tvdth the mo s I     ne r ent ne1ease date
     -    ID    KB 500317 3
     -    Relea  s e date    20210511

[+ d Done . D i s p let' ing 82 of the 82 vu lne ceb i l it ie s I ound .
```



Name	Date modified	Typ
Today (2)		
windows10.0-kb4601554-arm64-ndp48_23af11b83d550c30893e79e32ec069d2a15d5eea.msu	05-06-2021 12:36 PM	Mic
Symbols of gmail	05-06-2021 09:15 AM	File
Earlier this week (1)		
mad.pdf	03-06-2021 08:43 PM	PDF
Last month (2)		
exe files	11-05-2021 12:21 PM	File
ProcessExplorer	02-05-2021 09:23 AM	File
Earlier this year (2)		
Symbols	26-04-2021 09:53 AM	File
MyASUS	04-03-2021 12:14 PM	File
A long time ago (2)		
PDF and other files	15-12-2020 10:41 AM	File
_temp_matlab_R2020b_win64	29-11-2020 07:35 PM	File

Windows Update Standalone Installer

Windows Update Standalone Installer

The update is not applicable to your computer.

9 items | 1 item selected 41.6 MB |