Scan Report

July 25, 2023

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "UTC", which is abbreviated "UTC". The task was "Scan-Azure-Win10Vulnerable -Credentialed". The scan started at Tue Jul 25 05:38:08 2023 UTC and ended at Tue Jul 25 05:58:51 2023 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
10.0.0.5 windows10-vulne	2	4	1	0	0
Total: 1	2	4	1	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 7 results selected by the filtering described above. Before filtering there were 63 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
10.0.0.5 - windows10-vulne	SMB	Success	Protocol SMB, Port 445, User cybersuhanlab

2 Results per Host

2.1 10.0.0.5

Host scan start	Tue Jul 25 05:38:47 2023 UTC
Host scan end	Tue Jul 25 05:58:44 2023 UTC

Service (Port)	Threat Level
general/tcp	High
general/tcp	Medium
3389/tcp	Medium
135/tcp	Medium
general/icmp	Low

2.1.1 High general/tcp

High (CVSS: 7.8)
NVT: Windows IExpress Untrusted Search Path Vulnerability

Summary
This host has IExpress bundled with Microsoft Windows and is prone to an untrusted search path vulnerability.

Vulnerability Detection Result
```
Fixed version:      Workaround
File checked:       C:\Windows\system32\IEXPRESS.EXE
File version:       11.0.19041.1
```

Impact
Successful exploitation will allow an attacker to execute arbitrary code with the privilege of the user invoking a vulnerable self-extracting archive file.

Solution:
Solution type: Workaround
As a workaround save self-extracting archive files into a newly created directory, and confirm there are no unrelated files in the directory and make sure there are no suspicious files in the directory where self-extracting archive files are saved.

Affected Software/OS
IExpress bundled with Microsoft Windows

Vulnerability Insight
The flaw exists due to an untrusted search path error in self-extracting archive files created by IExpress bundled with Microsoft Windows.

Vulnerability Detection Method
Check for the presence of IExpress (IEXPRESS.EXE).
Details: `Windows IExpress Untrusted Search Path Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.813808
Version used: `2023-07-20T05:05:18Z`

References
```
cve: CVE-2018-0598
url: http://jvn.jp/en/jp/JVN72748502/index.html
url: https://blogs.technet.microsoft.com/srd/2018/04/04/triaging-a-dll-planting-
↪vulnerability
```

High (CVSS: 7.8)
NVT: Windows IExpress Untrusted Search Path Vulnerability

Summary

. . . continues on next page . . .

... continued from previous page ...

This host has IExpress bundled with Microsoft Windows and is prone to an untrusted search path vulnerability.

Vulnerability Detection Result

```
Fixed version:      Workaround
File checked:       C:\Windows\system32\IEXPRESS.EXE
File version:       11.0.19041.1
```

Impact

Successful exploitation will allow an attacker to execute arbitrary code with the privilege of the user invoking a vulnerable self-extracting archive file.

Solution:

Solution type: Workaround

As a workaround save self-extracting archive files into a newly created directory, and confirm there are no unrelated files in the directory and make sure there are no suspicious files in the directory where self-extracting archive files are saved.

Affected Software/OS

IExpress bundled with Microsoft Windows

Vulnerability Insight

The flaw exists due to an untrusted search path error in self-extracting archive files created by IExpress bundled with Microsoft Windows.

Vulnerability Detection Method

Check for the presence of IExpress (IEXPRESS.EXE).

Details: `Windows IExpress Untrusted Search Path Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.813808

Version used: `2023-07-20T05:05:18Z`

References

```
cve: CVE-2018-0598
url: http://jvn.jp/en/jp/JVN72748502/index.html
url: https://blogs.technet.microsoft.com/srd/2018/04/04/triaging-a-dll-planting-
↪vulnerability
```

[return to 10.0.0.5]

2.1.2 Medium general/tcp

Medium (CVSS: 6.9)
NVT: Microsoft Windows HID Functionality (Over USB) Code Execution Vulnerability (Jan 2011)

Summary
A USB device driver software is prone to a code execution vulnerability.

Vulnerability Detection Result
`File checked for existence: C:\Windows\system32\hidserv.dll`

Impact
Successful exploitation will allow user-assisted attackers to execute arbitrary programs via crafted USB data.

Solution:
Solution type: Workaround
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
A workaround is to introduce device filtering on the target host to only allow trusted USB devices to be enabled automatically. Once this workaround is in place an overwrite for this vulnerability can be created to mark it as a false positive.

Affected Software/OS
All Microsoft Windows systems with an enabled USB device driver and no local protection mechanism against the automatic enabling of additional Human Interface Device (HID).

Vulnerability Insight
The flaw is due to error in USB device driver (hidserv.dll), which does not properly warn the user before enabling additional Human Interface Device (HID) functionality.

Vulnerability Detection Method
Checks via SMB if a specific device driver (hidserv.dll) exists on the target system.
Details: `Microsoft Windows HID Functionality (Over USB) Code Execution Vulnerability (Ja.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.801581
Version used: `2023-01-12T10:12:15Z`

References
`cve: CVE-2011-0638`
`url: http://www.cs.gmu.edu/~astavrou/publications.html`
`url: http://news.cnet.com/8301-27080_3-20028919-245.html`
`url: http://www.blackhat.com/html/bh-dc-11/bh-dc-11-briefings.html#Stavrou`

Medium (CVSS: 6.9)
NVT: Microsoft Windows HID Functionality (Over USB) Code Execution Vulnerability (Jan 2011)

Summary
A USB device driver software is prone to a code execution vulnerability.

Vulnerability Detection Result
`File checked for existence: C:\Windows\system32\hidserv.dll`

Impact
Successful exploitation will allow user-assisted attackers to execute arbitrary programs via crafted USB data.

Solution:
Solution type: Workaround
No solution or patch was made available for at least one year since disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
A workaround is to introduce device filtering on the target host to only allow trusted USB devices to be enabled automatically. Once this workaround is in place an overwrite for this vulnerability can be created to mark it as a false positive.

Affected Software/OS
All Microsoft Windows systems with an enabled USB device driver and no local protection mechanism against the automatic enabling of additional Human Interface Device (HID).

Vulnerability Insight
The flaw is due to error in USB device driver (hidserv.dll), which does not properly warn the user before enabling additional Human Interface Device (HID) functionality.

Vulnerability Detection Method
Checks via SMB if a specific device driver (hidserv.dll) exists on the target system.
Details: `Microsoft Windows HID Functionality (Over USB) Code Execution Vulnerability (Ja.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.801581
Version used: `2023-01-12T10:12:15Z`

References
`cve: CVE-2011-0638`
`url: http://www.cs.gmu.edu/~astavrou/publications.html`
`url: http://news.cnet.com/8301-27080_3-20028919-245.html`
`url: http://www.blackhat.com/html/bh-dc-11/bh-dc-11-briefings.html#Stavrou`

[return to 10.0.0.5]

2.1.3 Medium 3389/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Summary
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result
```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and
↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c
↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1
↪.25623.1.0.802067) VT.
```

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2021-07-19T08:11:48Z`

References
```
cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
```

. . . continues on next page . . .

... continued from previous page ...

```
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

[return to 10.0.0.5]

2.1.4 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Vulnerability Detection Result

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49664/tcp
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.5[49664]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
     UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.5[49664]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.5[49664]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:10.0.0.5[49664]
     Annotation: KeyIso
Port: 49665/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.5[49665]
Port: 49666/tcp
     UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
     Endpoint: ncacn_ip_tcp:10.0.0.5[49666]
```

... continues on next page ...

... continued from previous page ...

```
      UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
      Endpoint: ncacn_ip_tcp:10.0.0.5[49666]
Port: 49667/tcp
      UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
      Endpoint: ncacn_ip_tcp:10.0.0.5[49667]
      Annotation: Event log TCPIP
Port: 49668/tcp
      UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1
      Endpoint: ncacn_ip_tcp:10.0.0.5[49668]
Port: 49669/tcp
      UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
      Endpoint: ncacn_ip_tcp:10.0.0.5[49669]
      UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
      Endpoint: ncacn_ip_tcp:10.0.0.5[49669]
      Named pipe : spoolss
      Win32 service or process : spoolsv.exe
      Description : Spooler service
      UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
      Endpoint: ncacn_ip_tcp:10.0.0.5[49669]
      UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
      Endpoint: ncacn_ip_tcp:10.0.0.5[49669]
      UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
      Endpoint: ncacn_ip_tcp:10.0.0.5[49669]
Port: 49670/tcp
      UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
      Endpoint: ncacn_ip_tcp:10.0.0.5[49670]
      Annotation: Remote Fw APIs
Port: 49681/tcp
      UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
      Endpoint: ncacn_ip_tcp:10.0.0.5[49681]
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution:
Solution type: Mitigation
Filter incoming traffic to this ports.

Vulnerability Detection Method
Details: DCE/RPC and MSRPC Services Enumeration Reporting
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: 2022-06-03T10:17:07Z

[return to 10.0.0.5]

2.1.5 Low general/icmp

Low (CVSS: 2.1) NVT: ICMP Timestamp Reply Information Disclosure
Summary The remote host responded to an ICMP timestamp request.

Vulnerability Detection Result
`The following response / ICMP packet has been received:`
`- ICMP Type: 14`
`- ICMP Code: 0`

Impact This information could theoretically be used to exploit weak time-based random number generators in other services.
Solution: **Solution type:** Mitigation Various mitigations are possible: - Disable the support for ICMP timestamp on the remote host completely - Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)
Vulnerability Insight The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.
Vulnerability Detection Method Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received. Details: `ICMP Timestamp Reply Information Disclosure` OID:1.3.6.1.4.1.25623.1.0.103190 Version used: `2023-05-11T09:09:33Z`

References
`cve: CVE-1999-0524`
`url: https://datatracker.ietf.org/doc/html/rfc792`
`url: https://datatracker.ietf.org/doc/html/rfc2780`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K14/0632`
`dfn-cert: DFN-CERT-2014-0658`

[return to 10.0.0.5]

This file was automatically generated.