

Network report

Report details

2022-11-16 11:18:18

Details:		Selection:	
Organization:	Mauritz Prive Test Omgeving	IPs:	10.0.10.1 - 10.0.10.254
Generated by:	MauritzTest MauritzTest	Tags:	
Report template:	Vulnerability manager network vulnerability template (by asset)	Host scanned:	254
Timezone:	Europe/Stockholm	Active hosts:	11
		Inactive hosts:	243
		Hosts matching filters:	8

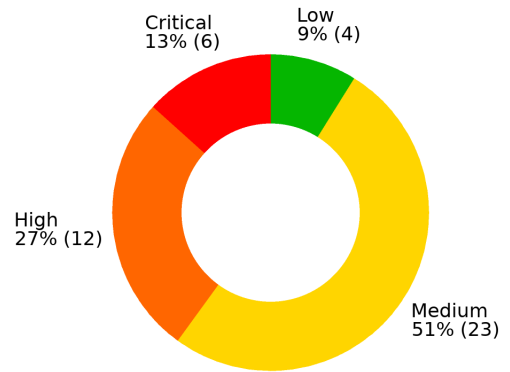
Vulnerability summary

[How is this calculated?](#)

Overall business risk

Medium

Severity levels

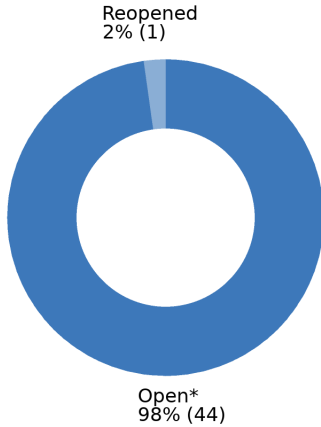


Vulnerabilities

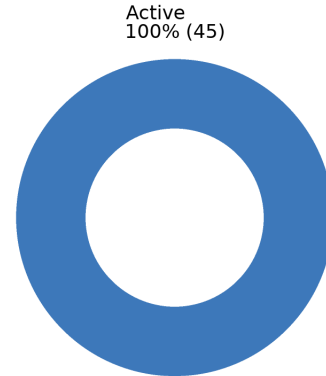
45

Excluding informational vulnerabilities

Status breakdown



State breakdown



Vulnerability list

Group by: host
Groups sorted by: IP
Sorting within each group: severity

Win7
10.0.10.91

Tags:

Business impact: Neutral

Critical

Operating System (OS) End of Life (EOL) Detection

New

HID:	HID-2-1-337131	First detected:	2022-10-24	Ticket:	Create ticket
CVSS v2 base:	10	Last detected:	2022-10-24	Published:	2013-03-05
CVSS v3.1 base:	10	Times detected:	1	Service modified:	2022-04-05
Operating system:	Windows 7 Professional 7601 Service Pack 1				
Port:					

CVE ID(s):

Impacted software:

Summary:

The Operating System (OS) on the remote host has reached the End of Life (EOL) and should not be used anymore.

Impact:

An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Insight:

Detection:

Checks if an EOL version of an OS is present on the target host.

Solution:

Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.

Exploits:

Ransomware:

References:

Result:

The "Windows 7" Operating System on the remote host has reached the end of life.

CPE: cpe:/o:microsoft:windows_7::sp1

Installed version,

build or SP: sp1

EOL date: 2020-01-14

EOL info: <https://support.microsoft.com/en-us/lifecycle/search?sort=PN&alpha=Windows%207&Filter=FilterNO>

High

SMBv1 enabled (Remote Check)

New

HID:	HID-2-1-374618	First detected:	2022-10-24	Ticket:	Create ticket
CVSS v2 base:	5.8	Last detected:	2022-10-24	Published:	2017-02-04
CVSS v3.1 base:	7.2	Times detected:	1	Service modified:	2022-11-07
Operating system:	Windows 7 Professional 7601 Service Pack 1				
Port:	445 (TCP)				

CVE ID(s):

Impacted software:

Summary:

The host has enabled SMBv1 for the SMB Server.

Impact:

Insight:

Detection:

Checks if SMBv1 is enabled for the SMB Server based on the information provided by the following VT:




- SMB Remote Version Detection (OID: 1.3.6.1.4.1.25623.1.0.807830).

Solution:

Exploits:

Ransomware:

References:

<https://support.microsoft.com/en-us/kb/204279> , <https://support.microsoft.com/en-us/kb/2696547> , <https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices> 

Result:

SMBv1 is enabled for the SMB Server

Medium

DCE/RPC and MSRPC Services Enumeration Reporting

New

HID:	HID-2-1-33182	First detected:	2022-10-24	Ticket:	Create ticket
CVSS v2 base:	5	Last detected:	2022-10-24	Published:	2017-01-12
CVSS v3.0 base:	0	Times detected:	1	Service modified:	2022-11-04
Operating system:	Windows 7 Professional 7601 Service Pack 1				
Port:	49152 (TCP)				

CVE ID(s):

Impacted software:

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. Many services depend on these ports to be open. If they are exposed attackers can use these ports to gather information. Please refer to solution for best practices related to DCE/RPC and MSRPC. This VT can be regarded as Risk acceptance(False Positive) if any such services are being used by host.

Impact:

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

Insight:

Detection:

Solution:

- > DCE/RPC should be updated to the latest version.
- > Allow only whitelisted local IP addresses to access port 135.
- > Filter incoming traffic to port 135.

Note: Solution needs to be manually verified.

Exploits:

Ransomware:

References:

Result:

The following DCE/RPC or MSRPC services are running on this port:

UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
Endpoint: ncacn_ip_tcp:10.0.10.91[49152]

Medium

DCE/RPC and MSRPC Services Enumeration Reporting

New

HID:	HID-2-1-33182	First detected:	2022-10-24	Ticket:	Create ticket
CVSS v2 base:	5	Last detected:	2022-10-24	Published:	2017-01-12
CVSS v3.0 base:	0	Times detected:	1	Service modified:	2022-11-04
Operating system:	Windows 7 Professional 7601 Service Pack 1				
Port:	49153 (TCP)				

CVE ID(s):

Impacted software:

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. Many services depend on these ports to be open. If they are exposed attackers can use these ports to gather information. Please refer to solution for best practices related to DCE/RPC and MSRPC. This VT can be regarded as Risk acceptance(False Positive) if any such services are being used by host.

Impact:

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

Insight:

Detection:

Solution:

- > DCE/RPC should be updated to the latest version.
- > Allow only whitelisted local IP addresses to access port 135.
- > Filter incoming traffic to port 135.

Note: Solution needs to be manually verified.

Exploits:

Ransomware:

References:

Result:

The following DCE/RPC or MSRPC services are running on this port:

UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
 Endpoint: ncacn_ip_tcp:10.0.10.91[49153]
 Named pipe : lsass
 Win32 service or process : lsass.exe
 Description : SAM access

UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 1
 Endpoint: ncacn_ip_tcp:10.0.10.91[49153]
 Annotation: KeyIso

Medium

DCE/RPC and MSRPC Services Enumeration Reporting

New

HID:	HID-2-1-33182	First detected:	2022-10-24	Ticket:	Create ticket
CVSS v2 base:	5	Last detected:	2022-10-24	Published:	2017-01-12
CVSS v3.0 base:	0	Times detected:	1	Service modified:	2022-11-04
Operating system:	Windows 7 Professional 7601 Service Pack 1				
Port:	49154 (TCP)				
CVE ID(s):					
Impacted software:					
<p>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. Many services depend on these ports to be open. If they are exposed attackers can use these ports to gather information. Please refer to solution for best practices related to DCE/RPC and MSRPC. This VT can be regarded as Risk acceptance(False Positive) if any such services are being used by host.</p>					
<p>Impact: An attacker may use this fact to gain more knowledge about the remote host.</p>					
Insight:					
Detection:					
<p>Solution:</p> <ul style="list-style-type: none"> -> DCE/RPC should be updated to the latest version. -> Allow only whitelisted local IP addresses to access port 135. -> Filter incoming traffic to port 135. <p>Note: Solution needs to be manually verified.</p>					
Exploits:					
Ransomware:					
References:					
<p>Result: The following DCE/RPC or MSRPC services are running on this port:</p> <p>UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1 Endpoint: ncacn_ip_tcp:10.0.10.91[49154] Annotation: Security Center</p> <p>UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1 Endpoint: ncacn_ip_tcp:10.0.10.91[49154] Annotation: NRP server endpoint</p> <p>UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:10.0.10.91[49154] Annotation: DHCP Client LRPC Endpoint</p> <p>... (showing first 500 characters)</p>					

Medium

DCE/RPC and MSRPC Services Enumeration Reporting

New

HID:	HID-2-1-33182	First detected:	2022-10-24	Ticket:	Create ticket
CVSS v2 base:	5	Last detected:	2022-10-24	Published:	2017-01-12
CVSS v3.0 base:	0	Times detected:	1	Service modified:	2022-11-04
Operating system:	Windows 7 Professional 7601 Service Pack 1				
Port:	49155 (TCP)				

CVE ID(s):

Impacted software:

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. Many services depend on these ports to be open. If they are exposed attackers can use these ports to gather information. Please refer to solution for best practices related to DCE/RPC and MSRPC. This VT can be regarded as Risk acceptance(False Positive) if any such services are being used by host.

Impact:

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

Insight:

Detection:

Solution:

- > DCE/RPC should be updated to the latest version.
- > Allow only whitelisted local IP addresses to access port 135.
- > Filter incoming traffic to port 135.

Note: Solution needs to be manually verified.

Exploits:

Ransomware:

References:

Result:

The following DCE/RPC or MSRPC services are running on this port:

UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1
Endpoint: ncacn_ip_tcp:10.0.10.91[49155]
Annotation: ApplInfo

UUID: 2eb08e3e-639f-4fba-97b1-14f878961076, version 1
Endpoint: ncacn_ip_tcp:10.0.10.91[49155]

UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
Endpoint: ncacn_ip_tcp:10.0.10.91[49155]
Annotation: IP Transition Configuration endpoint

UUID: 58e604e8-9adb-4d2e-a464-3... (showing first 500 characters)

Medium

DCE/RPC and MSRPC Services Enumeration Reporting

New

HID:	HID-2-1-33182	First detected:	2022-10-24	Ticket:	Create ticket
CVSS v2 base:	5	Last detected:	2022-10-24	Published:	2017-01-12
CVSS v3.0 base:	0	Times detected:	1	Service modified:	2022-11-04
Operating system:	Windows 7 Professional 7601 Service Pack 1				
Port:	49156 (TCP)				

CVE ID(s):

Impacted software:

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. Many services depend on these ports to be open. If they are exposed attackers can use these ports to gather information. Please refer to solution for best practices related to DCE/RPC and MSRPC. This VT can be regarded as Risk acceptance(False Positive) if any such services are being used by host.

Impact:

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

Insight:

Detection:

Solution:

- > DCE/RPC should be updated to the latest version.
- > Allow only whitelisted local IP addresses to access port 135.
- > Filter incoming traffic to port 135.

Note: Solution needs to be manually verified.

Exploits:

Ransomware:

References:

Result:

The following DCE/RPC or MSRPC services are running on this port:

UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
Endpoint: ncacn_ip_tcp:10.0.10.91[49156]

Medium

DCE/RPC and MSRPC Services Enumeration Reporting

New

HID:	HID-2-1-33182	First detected:	2022-10-24	Ticket:	Create ticket
CVSS v2 base:	5	Last detected:	2022-10-24	Published:	2017-01-12
CVSS v3.0 base:	0	Times detected:	1	Service modified:	2022-11-04
Operating system:	Windows 7 Professional 7601 Service Pack 1				
Port:	49161 (TCP)				

CVE ID(s):

Impacted software:

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. Many services depend on these ports to be open. If they are exposed attackers can use these ports to gather information. Please refer to solution for best practices related to DCE/RPC and MSRPC. This VT can be regarded as Risk acceptance(False Positive) if any such services are being used by host.

Impact:

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

Insight:

Detection:

Solution:

- > DCE/RPC should be updated to the latest version.
- > Allow only whitelisted local IP addresses to access port 135.
- > Filter incoming traffic to port 135.

Note: Solution needs to be manually verified.

Exploits:

Ransomware:

References:

Result:

The following DCE/RPC or MSRPC services are running on this port:

UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
Endpoint: ncacn_ip_tcp:10.0.10.91[49161]
Annotation: IPSec Policy agent endpoint
Named pipe : spoolss
Win32 service or process : spoolsv.exe
Description : Spooler service

UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
Endpoint: ncacn_ip_tcp:10.0.10.91[49161]
Annotation: Remote Fw APIs

Medium

DCE/RPC and MSRPC Services Enumeration Reporting

New

HID:	HID-2-1-33182	First detected:	2022-10-24	Ticket:	Create ticket
CVSS v2 base:	5	Last detected:	2022-10-24	Published:	2017-01-12
CVSS v3.0 base:	0	Times detected:	1	Service modified:	2022-11-04
Operating system:	Windows 7 Professional 7601 Service Pack 1				
Port:	135 (TCP)				
CVE ID(s):					
Impacted software:					
<p>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. Many services depend on these ports to be open. If they are exposed attackers can use these ports to gather information. Please refer to solution for best practices related to DCE/RPC and MSRPC. This VT can be regarded as Risk acceptance(False Positive) if any such services are being used by host.</p>					
<p>Impact: An attacker may use this fact to gain more knowledge about the remote host.</p>					
Insight:					
Detection:					
<p>Solution:</p> <ul style="list-style-type: none"> -> DCE/RPC should be updated to the latest version. -> Allow only whitelisted local IP addresses to access port 135. -> Filter incoming traffic to port 135. <p>Note: Solution needs to be manually verified.</p>					
Exploits:					
Ransomware:					
References:					

Result:

Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:

Port: 49152/tcp

UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
Endpoint: ncacn_ip_tcp:10.0.10.91[49152]

Port: 49153/tcp

UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
Endpoint: ncacn_ip_tcp:10.0.10.91[49153]
Named pipe : lsass
Win32 service or process : lsass.exe
Description : SAM access

UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 1
Endp... (showing first 500 characters)

Low TCP timestamps				New
HID:	HID-2-1-03447	First detected:	2022-10-24	Ticket: Create ticket
CVSS v2 base:	1.9	Last detected:	2022-10-24	Published: 2008-10-24
CVSS v3.0 base:	0	Times detected:	1	Service modified: 2020-08-24
Operating system:	Windows 7 Professional 7601 Service Pack 1			
Port:				
CVE ID(s):				
Impacted software: TCP implementations that implement RFC1323/RFC7323.				
Summary: The remote host implements TCP timestamps and therefore allows to compute the uptime.				
Impact: A side effect of this feature is that the uptime of the remote host can sometimes be computed.				
Insight: The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.				
Detection: Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.				

Solution:

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See the references for more information.

Exploits:**Ransomware:****References:**

<https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152> , <http://www.ietf.org/rfc/rfc7323.txt> , <http://www.ietf.org/rfc/rfc1323.txt> 

Result:

It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:

Packet 1: 373884

Packet 2: 373999

NOTEBOOK

10.0.10.88

Tags:

Business impact: Neutral

High SMBv1 enabled (Remote Check)

New

HID:	HID-2-1-374618	First detected:	2022-10-17	Ticket:	Create ticket
CVSS v2 base:	5.8	Last detected:	2022-10-17	Published:	2017-02-04
CVSS v3.1 base:	7.2	Times detected:	1	Service modified:	2022-11-07
Operating system:	Microsoft Windows				
Port:	445 (TCP)				

CVE ID(s):

Impacted software:

Summary:

The host has enabled SMBv1 for the SMB Server.

Impact:

Insight:

Detection:

Checks if SMBv1 is enabled for the SMB Server based on the information provided by the following VT:

- SMB Remote Version Detection (OID: 1.3.6.1.4.1.25623.1.0.807830).

Solution:

Exploits:

Ransomware:

References:

<https://support.microsoft.com/en-us/kb/204279> <https://support.microsoft.com/en-us/kb/2696547> , <https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices>

Result:

SMBv1 is enabled for the SMB Server

Medium DCE/RPC and MSRPC Services Enumeration Reporting

New

HID:	HID-2-1-33182	First detected:	2022-10-17	Ticket:	Create ticket
CVSS v2 base:	5	Last detected:	2022-10-17	Published:	2017-01-12
CVSS v3.0 base:	0	Times detected:	1	Service modified:	2022-11-04
Operating system:	Microsoft Windows				
Port:	135 (TCP)				

CVE ID(s):

Impacted software:

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. Many services depend on these ports to be open. If they are exposed attackers can use these ports to gather information. Please refer to solution for best practices related to DCE/RPC and MSRPC. This VT can be regarded as Risk acceptance(False Positive) if any such services are being used by host.

Impact:

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

Insight:**Detection:****Solution:**

- > DCE/RPC should be updated to the latest version.
- > Allow only whitelisted local IP addresses to access port 135.
- > Filter incoming traffic to port 135.

Note: Solution needs to be manually verified.

Exploits:**Ransomware:****References:****Result:**

Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:

Port: 49664/tcp

UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1

Endpoint: ncacn_ip_tcp:10.0.10.88[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:10.0.10.88[49664]

Annotation: Ngc Pop Key Service

UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b,... (showing first 500 characters)

MauritzLaptop_Wired

10.0.10.54

Tags:

Business impact: Neutral

Critical

Microsoft Windows Multiple Vulnerabilities - KB5017328

New

HID:	HID-2-1-5348441	First detected:	2022-10-24	Ticket:	#3
CVSS v2 base:	10	Last detected:	2022-10-24	Published:	2022-10-19
CVSS v3.1 base:	9.8	Times detected:	1	Service modified:	2022-10-19
Operating system:	Windows 10 Enterprise 21h2				
Port:					

CVE ID(s):

[CVE-2022-23960](#) [CVE-2022-26928](#) [CVE-2022-30170](#) [CVE-2022-30196](#) [CVE-2022-30200](#) [CVE-2022-34718](#) [CVE-2022-34719](#) [CVE-2022-34720](#) [CVE-2022-34721](#) [CVE-2022-34722](#) [CVE-2022-34723](#) [CVE-2022-34725](#) [CVE-2022-34726](#) [CVE-2022-34727](#) [CVE-2022-34728](#) [CVE-2022-34729](#) [CVE-2022-34730](#) [CVE-2022-34731](#) [CVE-2022-34732](#) [CVE-2022-34733](#) [CVE-2022-34734](#) [CVE-2022-35803](#) [CVE-2022-35831](#) [CVE-2022-35832](#) [CVE-2022-35833](#) [CVE-2022-35834](#) [CVE-2022-35835](#) [CVE-2022-35836](#) [CVE-2022-35837](#) [CVE-2022-35838](#) [CVE-2022-35840](#) [CVE-2022-35841](#) [CVE-2022-37954](#) [CVE-2022-37955](#) [CVE-2022-37956](#) [CVE-2022-37957](#) [CVE-2022-37958](#) [CVE-2022-37969](#) [CVE-2022-38004](#) [CVE-2022-38005](#) [CVE-2022-38006](#)

Impacted software:

Microsoft Windows 11 for ARM64-based Systems

Summary:

The Windows host is missing a security update and therefore is affected by multiple vulnerabilities.

Impact:

Successful exploitation will allow an attacker to run a remote code, perform privilege escalation and gain access to sensitive information.

Insight:

Among the most severe vulnerabilities affecting this host, we highlight the following:

- Certain Arm Cortex and Neoverse processors through 2022-03-08 do not properly restrict cache speculation, aka Spectre-BHB. An attacker can leverage the shared branch history in the Branch History Buffer (BHB) to influence mispredicted branches. Then, cache allocation can allow the attacker to obtain sensitive information. (CVE-2022-23960)
- Windows Photo Import API Elevation of Privilege Vulnerability (CVE-2022-26928)
- Windows Credential Roaming Service Elevation of Privilege Vulnerability (CVE-2022-30170)
- Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability (CVE-2022-37969) *(showing first 700 characters)*

Detection:

Checks if a vulnerable version is present on the target host.

Solution:

The vendor has released updates. Please see the reference for more information.

Exploits:

https://search.us-cert.gov/search?affiliate=cisa&sort_by=&query=CVE-2022-37969

Ransomware:

References:

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-23960> 

Result:

File checked: C:\Windows\system32\msctf.dll

File version: 10.0.22000.778


Vulnerable range: Less than 10.0.22000.978

Critical

Windows IExpress Untrusted Search Path Vulnerability

New

HID:	HID-2-1-047365	First detected:	2022-10-24	Ticket:	Create ticket
CVSS v2 base:	9.3	Last detected:	2022-10-24	Published:	2018-08-02
CVSS v3.0 base:	7.8	Times detected:	1	Service modified:	2021-06-24
Operating system:	Windows 10 Enterprise 21h2				
Port:					

CVE ID(s):[CVE-2018-0598](#) **Impacted software:**

IExpress bundled with Microsoft Windows

Summary:

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

Impact:

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

Insight:

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



Detection:

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

Solution:

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.

Exploits:**Ransomware:****References:**

<https://blogs.technet.microsoft.com/srd/2018/04/04/triaging-a-dll-planting-vulnerability>  ,
<http://jvn.jp/en/jp/JVN72748502/index.html> 

Result:

Fixed version: Workaround
File checked: C:\Windows\system32\IEXPRESS.EXE
File version: 11.0.22000.653

High

Oracle Java SE Security Update (jul2022) - Windows

New

HID:	HID-2-1-055646	First detected:	2022-10-24	Ticket:	Create ticket
CVSS v2 base:	7.8	Last detected:	2022-10-24	Published:	2022-07-25
CVSS v3.1 base:	9.8	Times detected:	1	Service modified:	2022-07-28
Operating system:	Windows 10 Enterprise 21h2				
Port:					

CVE ID(s):

[CVE-2022-21540](#) [CVE-2022-21541](#) [CVE-2022-21549](#) [CVE-2022-34169](#)

Impacted software:

Oracle Java SE version 7u343 (1.7.0.343) and earlier, 8u333 (1.8.0.333) and earlier, 11.x through 11.0.15.1, 17.x through 17.0.3.1, 18.x through 18.0.1.1 on Windows.

Summary:

Oracle Java SE is prone to multiple vulnerabilities.

Impact:

Successful exploitation will allow remote attacker to have an impact on confidentiality, integrity and availability.

Insight:

Multiple flaws are due to unspecified errors in 'Libraries', 'JAXP' and 'Hotspot' components.

Detection:

Checks if a vulnerable version is present on the target host.

Solution:

The vendor has released updates. Please see the references for more information.

Exploits:

Ransomware:

References:

<https://www.oracle.com/security-alerts/cpujul2022.html#AppendixJAVA>

Result:

Installed version: 1.8.0update_333
Fixed version: Apply the patch
Installation
path / port: C:\Program Files\Java\jre1.8.0_333

High

SMBv1 Client Detection

New

HID:	HID-2-1-044017	First detected:	2022-10-24	Ticket:	Create ticket
CVSS v2 base:	5.8	Last detected:	2022-10-24	Published:	2017-02-14
CVSS v3.1 base:	7.2	Times detected:	1	Service modified:	2022-11-07
Operating system:	Windows 10 Enterprise 21h2				
Port:					

CVE ID(s):

Impacted software:

Summary:

Detecting if SMBv1 is enabled for the SMB Client or not.

The script logs in via SMB, searches for key specific to the SMB Client in the registry and gets the value from the 'Start' string.

Impact:

Insight:

Detection:

Solution:

Exploits:

Ransomware:

References:

Result:

SMBv1 is enabled for the SMB Client

High

SMBv1 enabled (Local Windows Check)

New

HID:	HID-2-1-044011	First detected:	2022-10-24	Ticket:	Create ticket
CVSS v2 base:	5.8	Last detected:	2022-10-24	Published:	2017-02-15
CVSS v3.1 base:	7.2	Times detected:	1	Service modified:	2022-11-07
Operating system:	Windows 10 Enterprise 21h2				
Port:					

CVE ID(s):

Impacted software:

Summary:

The host has enabled SMBv1 for the SMB Client or Server.

Impact:

Insight:

Detection:

Checks if SMBv1 is enabled for the SMB Client or Server based on the information provided by the following two VTs:




- SMBv1 Client Detection (OID: 1.3.6.1.4.1.25623.1.0.810550)
- SMBv1 Server Detection (OID: 1.3.6.1.4.1.25623.1.0.810549).

Solution:

Exploits:

Ransomware:

References:

<https://support.microsoft.com/en-us/kb/204279> , <https://support.microsoft.com/en-us/kb/2696547> , <https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices> 

Result:


- SMBv1 is enabled for the SMB Client

Medium

PuTTY < 0.75 DoS Vulnerability

New

HID:	HID-2-1-342540	First detected:	2022-10-24	Ticket:	Create ticket
CVSS v2 base:	5	Last detected:	2022-10-24	Published:	2021-05-26
CVSS v3.1 base:	7.5	Times detected:	1	Service modified:	2021-08-24
Operating system:	Windows 10 Enterprise 21h2				
Port:					

CVE ID(s):
[CVE-2021-33500](#) 

Impacted software:
PuTTY before version 0.75.

Summary:
PuTTY is prone to a denial of service (DoS) vulnerability.

Impact:

Insight:
Remote servers are allowed to cause a denial of service (Windows GUI hang) by telling the PuTTY window to change its title repeatedly at high speed, which results in many SetWindowTextA or SetWindowTextW calls.

Detection:
Checks if a vulnerable version is present on the target host.

Solution:
Update to version 0.75 or later.

Exploits:

Ransomware:

References:
<https://www.chiark.greenend.org.uk/~sgtatham/putty/changes.html> 

Result:
Installed version: 0.74
Fixed version: 0.75
Installation
path / port: unknown

Medium

Source Routed Packets

Active

HID:	HID-2-1-34280	First detected:	2022-10-24	Ticket:	Create ticket
CVSS v2 base:	3.3	Last detected:	2022-10-24	Published:	2005-11-03
CVSS v3.0 base:	0	Times detected:	4	Service modified:	2021-01-20
Operating system:	Windows 10 Enterprise 21h2				
Port:					

CVE ID(s):

Impacted software:

Summary:

The remote host accepts loose source routed IP packets.
The feature was designed for testing purpose.

Impact:

An attacker may use it to circumvent poorly designed IP filtering and exploit another flaw. However, it is not dangerous by itself.

Worse, the remote host reverses the route when it answers to loose source routed TCP packets. This makes attacks easier.

Insight:

Detection:

Solution:

Drop source routed packets on this host or on other ingress routers or firewalls.

Exploits:

Ransomware:

References:

Result:

Medium

Relative IP Identification number change

Active

HID:	HID-2-1-33657	First detected:	2022-10-24	Ticket:	Create ticket
CVSS v2 base:	2.6	Last detected:	2022-10-24	Published:	2005-11-03
CVSS v3.0 base:	0	Times detected:	4	Service modified:	2020-08-24
Operating system:	Windows 10 Enterprise 21h2				
Port:					

CVE ID(s):

Impacted software:

Summary:

The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host.

Impact:

An attacker may use this feature to determine traffic patterns within your network. A few examples (not at all exhaustive) are:

1. A remote attacker can determine if the remote host sent a packet in reply to another request. Specifically, an attacker can use your server as an unwilling participant in a blind portscan of another network.
2. A remote attacker can roughly determine server requests at certain times of the day. For instance, if the server is sending much more traffic after business hours, the server may be a reverse proxy or other remote access device. An attacker can use this information to concentrate his/her efforts on the more critical machines.
3. ... (showing first 700 characters)

Insight:

Detection:

Solution:

Contact your vendor for a patch

Exploits:

Ransomware:

References:

Result:

The target host was found to be vulnerable

Low

TCP timestamps

Active

HID:	HID-2-1-03447	First detected:	2022-10-24	Ticket:	Create ticket
CVSS v2 base:	1.9	Last detected:	2022-10-24	Published:	2008-10-24
CVSS v3.0 base:	0	Times detected:	4	Service modified:	2020-08-24
Operating system:	Windows 10 Enterprise 21h2				
Port:					
CVE ID(s):					
Impacted software: TCP implementations that implement RFC1323/RFC7323.					
Summary: The remote host implements TCP timestamps and therefore allows to compute the uptime.					
Impact: A side effect of this feature is that the uptime of the remote host can sometimes be computed.					
Insight: The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.					
Detection: Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.					
Solution: To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.					
Exploits:					
Ransomware:					
References: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152 , http://www.ietf.org/rfc/rfc7323.txt , http://www.ietf.org/rfc/rfc1323.txt					
Result: It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 1360858 Packet 2: 1362021					

10.0.10.47

10.0.10.47

Tags:

Business impact: Neutral

Low TCP timestamps

New

HID:	HID-2-1-03447	First detected:	2022-10-13	Ticket:	Create ticket
CVSS v2 base:	1.9	Last detected:	2022-10-13	Published:	2008-10-24
CVSS v3.0 base:	0	Times detected:	1	Service modified:	2020-08-24
Operating system:	unknown				
Port:					

CVE ID(s):

Impacted software:

TCP implementations that implement RFC1323/RFC7323.

Summary:

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Impact:

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Insight:

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Detection:

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

Solution:

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See the references for more information.

Exploits:

Ransomware:

References:

<https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152> , <http://www.ietf.org/rfc/rfc7323.txt> , <http://www.ietf.org/rfc/rfc1323.txt>

Result:

It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:

Packet 1: 1026765

Packet 2: 1028064

10.0.10.46

10.0.10.46

Tags:

Business impact: Neutral


High

libupnp < 1.14.6 DNS Rebind Vulnerability (GHSA-6hqq-w3jq-9fhg)

New

HID:	HID-2-1-379371	First detected:	2022-10-13	Ticket:	#4
CVSS v2 base:	7.5	Last detected:	2022-10-13	Published:	2021-04-22
CVSS v3.1 base:	9.8	Times detected:	1	Service modified:	2021-08-17
Operating system:	unknown				
Port:	49152 (TCP)				

CVE ID(s):

[CVE-2021-29462](#) 

Impacted software:

libupnp prior to version 1.14.6.

Summary:

libupnp is prone to a DNS rebind vulnerability.

Impact:

This vulnerability can be used to exfiltrate the content of the media files exposed by a UPnP AV MediaServer server. Moreover, it could be possible to delete or upload files if this is enabled in the server configuration.

Insight:

The server part of pupnp (libupnp) is vulnerable to DNS-rebinding attacks because it does not check the value of the Host header.

A remote web server can exploit this vulnerability to trick the user browser into triggering actions on the local UPnP services implemented using this library. Depending on the affected service, this could be used for data exfiltration, data tempering, etc.

Detection:

Checks if a vulnerable version is present on the target host.

Solution:

Update to version 1.14.6 or later.

Exploits:

Ransomware:

References:

<https://github.com/pupnp/pupnp/security/advisories/GHSA-6hqq-w3jq-9fhg> 

Result:

Installed version: 1.6.19

Fixed version: 1.14.6

Installation


path / port: 49152/tcp

Medium

libupnp <= 1.12.1 DoS Vulnerability

New

HID:	HID-2-1-347156	First detected:	2022-10-13	Ticket:	Create ticket
CVSS v2 base:	5	Last detected:	2022-10-13	Published:	2020-06-08
CVSS v3.1 base:	7.5	Times detected:	1	Service modified:	2021-07-07
Operating system:	unknown				
Port:	49152 (TCP)				

CVE ID(s):
[CVE-2020-13848](#) 

Impacted software:
libupnp through version 1.12.1.

Summary:
libupnp is prone to a denial of service (DoS) vulnerability.

Impact:
Successful exploitation would allow an attacker to crash the service.

Insight:
The vulnerability can be exploited via a crafted SSDP message due to a NULL pointer dereference in the functions FindServiceControlURLPath and FindServiceEventURLPath in genlib/service_table/service_table.c.

Detection:
Checks if a vulnerable version is present on the target host.

Solution:
Update to version 1.12.2 or later.

Exploits:

Ransomware:

References:
<https://github.com/pupnp/pupnp/commit/c805c1de1141cb22f74c0d94dd5664bda37398e0> ,
<https://github.com/pupnp/pupnp/issues/177> 

Result:
Installed version: 1.6.19
Fixed version: 1.12.2
Installation
path / port: 49152/tcp

Low

TCP timestamps

New

HID:	HID-2-1-03447	First detected:	2022-10-13	Ticket:	Create ticket
CVSS v2 base:	1.9	Last detected:	2022-10-13	Published:	2008-10-24
CVSS v3.0 base:	0	Times detected:	1	Service modified:	2020-08-24
Operating system:	unknown				
Port:					

CVE ID(s):**Impacted software:**

TCP implementations that implement RFC1323/RFC7323.

Summary:

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Impact:

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Insight:

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Detection:

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

Solution:

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See the references for more information.

Exploits:**Ransomware:****References:**

<https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152> , <http://www.ietf.org/rfc/rfc7323.txt> , <http://www.ietf.org/rfc/rfc1323.txt>

Result:

It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:

Packet 1: 1591150236

Packet 2: 1591166212

DESKTOP-87LLU4C

10.0.10.45

Tags:

Business impact: Neutral

Critical	Microsoft Windows Unquoted Path Vulnerability (SMB Login)			Active	
HID:	HID-2-1-331860	First detected:	2022-10-25	Ticket:	Create ticket
CVSS v2 base:	9.3	Last detected:	2022-10-25	Published:	2018-03-23
CVSS v3.0 base:	7.8	Times detected:	2	Service modified:	2022-09-16
Operating system:	Windows 10 Pro 21h1				
Port:					

CVE ID(s):

[CVE-2005-2936](#) [CVE-2007-5618](#) [CVE-2009-2761](#) [CVE-2012-4350](#) [CVE-2013-0513](#) [CVE-2013-1092](#) [CVE-2013-1609](#) [CVE-2013-1610](#) [CVE-2013-2151](#) [CVE-2013-2152](#) [CVE-2013-2176](#) [CVE-2013-2231](#) [CVE-2013-5011](#) [CVE-2013-6182](#) [CVE-2013-6773](#) [CVE-2014-0759](#) [CVE-2014-4634](#) [CVE-2014-5455](#) [CVE-2014-9646](#) [CVE-2015-0884](#) [CVE-2015-1484](#) [CVE-2015-2789](#) [CVE-2015-3987](#) [CVE-2015-4173](#) [CVE-2015-7866](#) [CVE-2015-8156](#) [CVE-2015-8988](#) [CVE-2016-15003](#) [CVE-2016-3161](#) [CVE-2016-4158](#) [CVE-2016-5793](#) [CVE-2016-5852](#) [CVE-2016-6803](#) [CVE-2016-6935](#) [CVE-2016-7165](#) [CVE-2016-8102](#) [CVE-2016-8225](#) [CVE-2016-8769](#) [CVE-2016-9356](#) [CVE-2017-1000475](#) [CVE-2017-12730](#) [CVE-2017-14019](#) [CVE-2017-14030](#) [CVE-2017-15383](#) [CVE-2017-3005](#) [CVE-2017-3141](#) [CVE-2017-3751](#) [CVE-2017-3756](#) [CVE-2017-3757](#) [CVE-2017-5873](#) [CVE-2017-6005](#) [CVE-2017-7180](#) [CVE-2017-9247](#) [CVE-2017-9644](#) [CVE-2018-0594](#) [CVE-2018-0595](#) [CVE-2018-11063](#) [CVE-2018-20341](#) [CVE-2018-2406](#) [CVE-2018-3668](#) [CVE-2018-3683](#) [CVE-2018-3684](#) [CVE-2018-3687](#) [CVE-2018-3688](#) [CVE-2018-5470](#) [CVE-2018-6016](#) [CVE-2018-6321](#) [CVE-2018-6384](#) [CVE-2019-11093](#) [CVE-2019-14599](#) [CVE-2019-14685](#) [CVE-2019-17658](#) [CVE-2019-20362](#) [CVE-2019-7201](#) [CVE-2019-7590](#) [CVE-2020-0507](#) [CVE-2020-0546](#) [CVE-2020-13884](#) [CVE-2020-15261](#) [CVE-2020-22809](#) [CVE-2020-28209](#) [CVE-2020-35152](#) [CVE-2020-5147](#) [CVE-2020-5569](#) [CVE-2020-7252](#) [CVE-2020-7316](#) [CVE-2020-7331](#) [CVE-2020-8326](#) [CVE-2020-9292](#) [CVE-2021-0112](#) [CVE-2021-21078](#) [CVE-2021-23197](#) [CVE-2021-23879](#) [CVE-2021-25269](#) [CVE-2021-27608](#) [CVE-2021-29218](#) [CVE-2021-33095](#) [CVE-2021-35230](#) [CVE-2021-35231](#) [CVE-2021-35469](#) [CVE-2021-37363](#) [CVE-2021-37364](#) [CVE-2021-42563](#) [CVE-2021-43454](#) [CVE-2021-43455](#) [CVE-2021-43456](#) [CVE-2021-43457](#) [CVE-2021-43458](#) [CVE-2021-43460](#) [CVE-2021-43463](#) [CVE-2021-45819](#) [CVE-2021-46443](#) [CVE-2022-2147](#) [CVE-2022-23909](#) [CVE-2022-25031](#) [CVE-2022-26634](#) [CVE-2022-27050](#) [CVE-2022-27052](#) [CVE-2022-27088](#) [CVE-2022-27089](#) [CVE-2022-27094](#) [CVE-2022-27095](#) [CVE-2022-29320](#) [CVE-2022-31591](#) [CVE-2022-33035](#) [CVE-2022-35292](#) [CVE-2022-35899](#)

Impacted software:

Software installing an 'Uninstall' registry entry or 'Service' on Microsoft Windows using an unquoted path containing at least one whitespace.

Summary:

The script tries to detect Windows 'Uninstall' registry entries and 'Services' using an unquoted path containing at least one whitespace.

Impact:

A local attacker could gain elevated privileges by inserting an executable file in the path of the affected service or uninstall entry.

Insight:

If the path contains spaces and is not surrounded by quotation marks, the Windows API has to guess where to find the referenced program. If e.g. a service is using the following unquoted path:

C:\Program Files\Folder\service.exe

then a start of the service would first try to run:

C:\Program.exe

and if not found:

C:\Program Files\Folder\service.exe

afterwards. In this example the behavior allows a local attacker with low privileges and write permissions on C:\ to place a malicious Program.exe which is then executed on a service/host restart or during the uninstallation of a software.

NOTE: Currently only 'Services' using an unquoted path are reported as a vulnerab ... (showing first 700 characters)





Detection:**Solution:**

Either put the listed vulnerable paths in quotation by manually using the onboard Registry editor or contact your vendor to get an update for the specified software that fixes this vulnerability.

Exploits:

<https://www.exploit-db.com/exploits/34037> , <https://www.exploit-db.com/exploits/36390> , <https://www.exploit-db.com/exploits/40807> , <https://www.exploit-db.com/exploits/42121> , <https://www.exploit-db.com/exploits/42141> , <https://www.exploit-db.com/exploits/42542> , <https://www.exploit-db.com/exploits/49925> , <https://www.exploit-db.com/exploits/50212> , <https://www.exploit-db.com/exploits/50852> , <https://www.exploit-db.com/exploits/50985> 

Ransomware:**References:**

<https://blogs.technet.microsoft.com/srd/2018/04/04/triaging-a-dll-planting-vulnerability> , <https://www.tecklyfe.com/remediation-microsoft-windows-unquoted-service-path-enumeration-vulnerability/> , <http://www.ryanandjeffshow.com/blog/2013/04/11/powershell-fixing-unquoted-service-paths-complete/> , <https://gallery.technet.microsoft.com/scriptcenter/Windows-Unquoted-Service-190f0341#content> 

Result:

The following 'Uninstall' registry entries are using an 'unquoted' path:

Key|Value

SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Capture|C:\Program Files\Logitech\LogiCapture\uninstaller.exe

SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\OneDriveSetup.exe|C:\Program Files\Microsoft

OneDrive\22.207.1002.0003\OneDriveSetup.exe /uninstall /allusers

SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SteelSeries GG|C:\Program Files\SteelSeries\GG\uninst.exe

SoftwareWow6432Node\Microso... (showing first 500 characters)

Critical

Windows IExpress Untrusted Search Path Vulnerability

Active

HID:	HID-2-1-047365	First detected:	2022-10-25	Ticket:	Create ticket
CVSS v2 base:	9.3	Last detected:	2022-10-25	Published:	2018-08-02
CVSS v3.0 base:	7.8	Times detected:	2	Service modified:	2021-06-24
Operating system:	Windows 10 Pro 21h1				
Port:					

CVE ID(s):[CVE-2018-0598](#) **Impacted software:**

IExpress bundled with Microsoft Windows

Summary:

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

Impact:

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

Insight:

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

Detection:

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

Solution:

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.

Exploits:**Ransomware:****References:**

<https://blogs.technet.microsoft.com/srd/2018/04/04/triaging-a-dll-planting-vulnerability>  ,
<http://jvn.jp/en/jp/JVN72748502/index.html> 

Result:

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

High

Microsoft Windows HID Functionality (Over USB) Code Execution Vulnerability

Active

HID:	HID-2-1-035048	First detected:	2022-10-25	Ticket:	Create ticket
CVSS v2 base:	6.9	Last detected:	2022-10-25	Published:	2011-01-31
CVSS v3.0 base:	0	Times detected:	2	Service modified:	2022-07-26
Operating system:	Windows 10 Pro 21h1				
Port:					

CVE ID(s):

[CVE-2011-0638](#) 

Impacted software:

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).

Summary:

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

Impact:

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

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.

Detection:

Solution:

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.

Exploits:

Ransomware:

References:

Result:

File checked for existence: C:\Windows\system32\hidserv.dll

High

Oracle VirtualBox Security Update(oct2022) - Windows

Active

HID:	HID-2-1-050040	First detected:	2022-10-25	Ticket:	#5
CVSS v2 base:	6.5	Last detected:	2022-10-25	Published:	2022-10-19
CVSS v3.0 base:	0	Times detected:	2	Service modified:	2022-10-20
Operating system:	Windows 10 Pro 21h1				
Port:					

CVE ID(s):

[CVE-2022-21620](#) [CVE-2022-21621](#) [CVE-2022-21627](#) [CVE-2022-39421](#) [CVE-2022-39424](#) [CVE-2022-39425](#) [CVE-2022-39426](#) [CVE-2022-39427](#)

Impacted software:

VirtualBox versions 6.1.x prior to 6.1.40 on Windows.

Summary:

Oracle VM VirtualBox is prone to multiple vulnerabilities.

Impact:

Successful exploitation will allow an attacker to have an impact on confidentiality, integrity and availability.

Insight:

Multiple flaws exist due to multiple errors in 'Core' component.

Detection:

Checks if a vulnerable version is present on the target host.

Solution:

Upgrade to Oracle VirtualBox version 6.1.40 or later. Please see the references for more information.

Exploits:

Ransomware:

References:

<https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixJAVA>

Result:

Installed version: 6.1.38

Fixed version: 6.1.40

Installation

path / port: C:\Program Files\Oracle\VirtualBox\

High

SMBv1 Client Detection

Active

HID:	HID-2-1-044017	First detected:	2022-10-25	Ticket:	Create ticket
CVSS v2 base:	5.8	Last detected:	2022-10-25	Published:	2017-02-14
CVSS v3.1 base:	7.2	Times detected:	2	Service modified:	2022-11-07
Operating system:	Windows 10 Pro 21h1				
Port:					

CVE ID(s):

Impacted software:

Summary:

Detecting if SMBv1 is enabled for the SMB Client or not.

The script logs in via SMB, searches for key specific to the SMB Client in the registry and gets the value from the 'Start' string.

Impact:

Insight:

Detection:

Solution:

Exploits:

Ransomware:

References:

Result:

SMBv1 is enabled for the SMB Client

High

SMBv1 enabled (Local Windows Check)

Active

HID:	HID-2-1-044011	First detected:	2022-10-25	Ticket:	Create ticket
CVSS v2 base:	5.8	Last detected:	2022-10-25	Published:	2017-02-15
CVSS v3.1 base:	7.2	Times detected:	2	Service modified:	2022-11-07
Operating system:	Windows 10 Pro 21h1				
Port:					

CVE ID(s):

Impacted software:

Summary:

The host has enabled SMBv1 for the SMB Client or Server.

Impact:

Insight:

Detection:

Checks if SMBv1 is enabled for the SMB Client or Server based on the information provided by the following two VTs:




- SMBv1 Client Detection (OID: 1.3.6.1.4.1.25623.1.0.810550)
- SMBv1 Server Detection (OID: 1.3.6.1.4.1.25623.1.0.810549).

Solution:

Exploits:

Ransomware:

References:

<https://support.microsoft.com/en-us/kb/204279> , <https://support.microsoft.com/en-us/kb/2696547> , <https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices> 

Result:

- SMBv1 is enabled for the SMB Server
- SMBv1 is enabled for the SMB Client

High

SMBv1 enabled (Remote Check)

Active

HID:	HID-2-1-374618	First detected:	2022-10-25	Ticket:	Create ticket
CVSS v2 base:	5.8	Last detected:	2022-10-25	Published:	2017-02-04
CVSS v3.1 base:	7.2	Times detected:	2	Service modified:	2022-11-07
Operating system:	Windows 10 Pro 21h1				
Port:	445 (TCP)				

CVE ID(s):

Impacted software:

Summary:

The host has enabled SMBv1 for the SMB Server.

Impact:

Insight:

Detection:

Checks if SMBv1 is enabled for the SMB Server based on the information provided by the following VT:




- SMB Remote Version Detection (OID: 1.3.6.1.4.1.25623.1.0.807830).

Solution:

Exploits:

Ransomware:


References:

<https://support.microsoft.com/en-us/kb/204279> , <https://support.microsoft.com/en-us/kb/2696547> , <https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices> 

Result:

SMBv1 is enabled for the SMB Server

High		SMBv1 Server Detection		Active	
HID:	HID-2-1-044006	First detected:	2022-10-25	Ticket:	Create ticket
CVSS v2 base:	5.8	Last detected:	2022-10-25	Published:	2017-02-14
CVSS v3.1 base:	7.2	Times detected:	2	Service modified:	2022-11-07
Operating system:	Windows 10 Pro 21h1				
Port:					
CVE ID(s):					
Impacted software:					
Summary: Detecting if SMBv1 is enabled for the SMB Server or not. The script logs in via SMB, searches for key specific to the SMB Server in the registry and gets the value from the 'SMB1' string.					
Impact:					
Insight:					
Detection:					
Solution:					
Exploits:					
Ransomware:					
References:					
Result: SMBv1 is enabled for the SMB Server					

Medium		Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)		Active	
HID:	HID-2-1-341307	First detected:	2022-10-13	Ticket:	Create ticket
CVSS v2 base:	5	Last detected:	2022-10-25	Published:	2021-12-16
CVSS v3.1 base:	7.5	Times detected:	9	Service modified:	2021-12-17
Operating system:	Windows 10 Pro 21h1				
Port:	3389 (TCP)				
CVE ID(s): CVE-2002-20001 					
Impacted software:					
Summary: The remote SSL/TLS server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange algorithms and thus could be prone to a denial of service (DoS) vulnerability.					
Impact:					

Insight:

The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.

Detection:

Checks the supported cipher suites of the remote SSL/TLS server.

Solution:

- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered.

- Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For Postfix this limit can be configured via 'smtpd_client_new_tls_session_rate_limit' option, for other products please refer to the manual of the product in question on configuration possibilities.

Exploits:**Ransomware:****References:**

<https://github.com/Balasys/dheater>  , https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol 

Result:

'DHE' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Medium

DCE/RPC and MSRPC Services Enumeration Reporting

Reopened

HID:	HID-2-1-33182	First detected:	2022-10-17	Ticket:	Create ticket
CVSS v2 base:	5	Last detected:	2022-10-25	Published:	2017-01-12
CVSS v3.0 base:	0	Times detected:	5	Service modified:	2022-11-04
Operating system:	Windows 10 Pro 21h1				
Port:	135 (TCP)				

CVE ID(s):

Impacted software:

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. Many services depend on these ports to be open. If they are exposed attackers can use these ports to gather information. Please refer to solution for best practices related to DCE/RPC and MSRPC. This VT can be regarded as Risk acceptance(False Positive) if any such services are being used by host.

Impact:

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

Insight:

Detection:

Solution:

- > DCE/RPC should be updated to the latest version.
- > Allow only whitelisted local IP addresses to access port 135.
- > Filter incoming traffic to port 135.

Note: Solution needs to be manually verified.

Exploits:

Ransomware:

References:

Result:

Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:

Port: 49664/tcp

UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
Endpoint: ncacn_ip_tcp:10.0.10.45[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:10.0.10.45[49664]
Annotation: Ngc Pop Key Service

UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b,... (showing first 500 characters)

Medium

Oracle Java SE Security Update (oct2022) 01 - Windows

Active

HID:	HID-2-1-050046	First detected:	2022-10-25	Ticket:	Create ticket
CVSS v2 base:	5	Last detected:	2022-10-25	Published:	2022-10-19
CVSS v3.0 base:	0	Times detected:	2	Service modified:	2022-10-20
Operating system:	Windows 10 Pro 21h1				
Port:					

CVE ID(s):

[CVE-2022-21619](#) [CVE-2022-21624](#) [CVE-2022-21628](#)

Impacted software:

Oracle Java SE version 8u341 and earlier,
11.x through 11.0.16.1, 17.x through 17.0.4.1, 19 on Windows.

Summary:

Oracle Java SE is prone to multiple vulnerabilities.

Impact:

Successful exploitation will allow remote attacker to have an impact on integrity and availability.

Insight:

Multiple flaws exist due to multiple errors in components 'JNDI', 'Security' and 'JNDI'.

Detection:

Checks if a vulnerable version is present on the target host.

Solution:

The vendor has released updates. Please see the references for more information.

Exploits:



Ransomware:

References:

<https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixJAVA>

Result:

Installed version: 1.8.0update_341
Fixed version: Apply the patch
Installation
path / port: C:\Program Files\Java\jre1.8.0_341

Medium Oracle Java SE Security Update (oct2022) 04 - Windows		Active	
HID:	HID-2-1-050050	First detected:	2022-10-25
CVSS v2 base:	5	Last detected:	2022-10-25
CVSS v3.0 base:	0	Times detected:	2
Operating system:	Windows 10 Pro 21h1	Ticket:	Create ticket
Port:		Published:	2022-10-19
		Service modified:	2022-10-20
CVE ID(s): CVE-2022-21626 			
Impacted software: Oracle Java SE version 8u341 and earlier, 11.x through 11.0.16.1 on Windows.			
Summary: Oracle Java SE is prone to multiple vulnerabilities.			
Impact: Successful exploitation will allow remote attacker to have an impact on availability.			
Insight: The flaw exists due to an error in component 'Security'.			
Detection: Checks if a vulnerable version is present on the target host.			
Solution: The vendor has released updates. Please see the references for more information.			
Exploits:			
Ransomware:			
References: https://www.oracle.com/security-alerts/cpuoct2022.html#AppendixJAVA 			
Result: Installed version: 1.8.0update_341 Fixed version: Apply the patch Installation path / port: C:\Program Files\Java\jre1.8.0_341			
Medium SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection		Active	
HID:	HID-2-1-341731	First detected:	2022-10-17
CVSS v2 base:	4.3	Last detected:	2022-10-25
CVSS v3.0 base:	0	Times detected:	7
Operating system:	Windows 10 Pro 21h1	Ticket:	Create ticket
Port:	3389 (TCP)	Published:	2021-03-25
		Service modified:	2021-07-19

CVE ID(s):

[CVE-2011-3389](#)  [CVE-2015-0204](#) 

Impacted software:

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

Summary:

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

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.

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)


Detection:

Check the used TLS protocols of the services provided by this system.

Solution:

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.

Exploits:**Ransomware:****References:**

<https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014> , <https://web.archive.org/web/20201108095603/https://censys.io/blog/freak> , <https://vnhacker.blogspot.com/2011/09/beast.html> , <https://datatracker.ietf.org/doc/rfc8996/> , <https://bettercrypto.org/> , <https://ssl-config.mozilla.org/> 

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 can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

10.0.10.12

10.0.10.12

Tags:

Business impact: Neutral

Medium

Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)

New

HID:	HID-2-1-341396	First detected:	2022-10-13	Ticket:	Create ticket
CVSS v2 base:	5	Last detected:	2022-10-13	Published:	2021-12-16
CVSS v3.1 base:	7.5	Times detected:	1	Service modified:	2021-12-17
Operating system:	unknown				
Port:	22 (TCP)				

CVE ID(s):

[CVE-2002-20001](#) 

Impacted software:

Summary:

The remote SSH server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange (KEX) algorithms and thus could be prone to a denial of service (DoS) vulnerability.

Impact:

Insight:

The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.

Detection:

Checks the supported KEX algorithms of the remote SSH server.

Solution:

- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered.
- Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For OpenSSH this limit can be configured via the 'MaxStartups' option, for other products please refer to the manual of the product in question on configuration possibilities.

Exploits:

Ransomware:

References:

<https://github.com/Balasys/dheater>  , https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol 

Result:

The remote SSH server supports the following DHE KEX algorithm(s):

diffie-hellman-group14-sha1
diffie-hellman-group14-sha256

Medium

Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)

New

HID:	HID-2-1-341307	First detected:	2022-10-13	Ticket:	Create ticket
CVSS v2 base:	5	Last detected:	2022-10-13	Published:	2021-12-16
CVSS v3.1 base:	7.5	Times detected:	1	Service modified:	2021-12-17
Operating system:	unknown				
Port:	8443 (TCP)				

CVE ID(s):

[CVE-2002-20001](#) 

Impacted software:**Summary:**

The remote SSL/TLS server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange algorithms and thus could be prone to a denial of service (DoS) vulnerability.

Impact:**Insight:**

The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.

Detection:



Checks the supported cipher suites of the remote SSL/TLS server.

Solution:

- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered.

- Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For Postfix this limit can be configured via 'smtpd_client_new_tls_session_rate_limit' option, for other products please refer to the manual of the product in question on configuration possibilities.

Exploits:**Ransomware:****References:**

<https://github.com/Balasy/dheater> , https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol 

Result:

'DHE' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Medium Weak Host Key Algorithm(s) (SSH) New

HID:	HID-2-1-341144	First detected:	2022-10-13	Ticket:	Create ticket
CVSS v2 base:	4.6	Last detected:	2022-10-13	Published:	2021-09-20
CVSS v3.1 base:	5.3	Times detected:	1	Service modified:	2021-11-24
Operating system:	unknown				
Port:	22 (TCP)				

CVE ID(s):

Impacted software:

Summary:
The remote SSH server is configured to allow / support weak host key algorithm(s).

Impact:

Insight:

Detection:
Checks the supported host key algorithms of the remote SSH server.

Currently weak host key algorithms are defined as the following:

- ssh-dss: Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)

Solution:
Disable the reported weak host key algorithm(s).

Exploits:

Ransomware:

References:

Result:
The remote SSH server supports the following weak host key algorithm(s):

host key algorithm	Description
ssh-dss	Digital Signature Algorithm (DSA) / Digital Signature Standard (DSS)

10.0.10.1

10.0.10.1

Tags:

Business impact: Neutral

Critical Operating System (OS) End of Life (EOL) Detection

New

HID:	HID-2-1-337131	First detected:	2022-10-13	Ticket:	Create ticket
CVSS v2 base:	10	Last detected:	2022-10-13	Published:	2013-03-05
CVSS v3.1 base:	10	Times detected:	1	Service modified:	2022-04-05
Operating system:	unknown				
Port:					

CVE ID(s):

Impacted software:

Summary:

The Operating System (OS) on the remote host has reached the End of Life (EOL) and should not be used anymore.

Impact:

An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Insight:

Detection:

Checks if an EOL version of an OS is present on the target host.

Solution:

Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.

Exploits:

Ransomware:

References:

Result:

The "Debian GNU/Linux" Operating System on the remote host has reached the end of life.

CPE: cpe:/o:debian:debian_linux:9

Installed version,




build or SP: 9

EOL date: 2022-06-30

EOL info: https://en.wikipedia.org/wiki/List_of_Debian_releases#Release_table

Medium Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)

New


HID:	HID-2-1-341396	First detected:	2022-10-13	Ticket:	Create ticket
CVSS v2 base:	5	Last detected:	2022-10-13	Published:	2021-12-16
CVSS v3.1 base:	7.5	Times detected:	1	Service modified:	2021-12-17
Operating system:	unknown				
Port:	22 (TCP)				
CVE ID(s):					
CVE-2002-20001 					
Impacted software:					
Summary:					
The remote SSH server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange (KEX) algorithms and thus could be prone to a denial of service (DoS) vulnerability.					
Impact:					
Insight:					
The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.					
Detection:					
Checks the supported KEX algorithms of the remote SSH server.					
Solution:					
- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered.					
- Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For OpenSSH this limit can be configured via the 'MaxStartups' option, for other products please refer to the manual of the product in question on configuration possibilities.					
Exploits:					
Ransomware:					
References:					
https://github.com/Balasys/dheater  , https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol 					
Result:					
The remote SSH server supports the following DHE KEX algorithm(s):					
diffie-hellman-group14-sha1					
diffie-hellman-group14-sha256					
diffie-hellman-group16-sha512					
diffie-hellman-group18-sha512					
diffie-hellman-group-exchange-sha256					

Medium

Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)

New

HID:	HID-2-1-341307	First detected:	2022-10-13	Ticket:	Create ticket
CVSS v2 base:	5	Last detected:	2022-10-13	Published:	2021-12-16
CVSS v3.1 base:	7.5	Times detected:	1	Service modified:	2021-12-17
Operating system:	unknown				
Port:	443 (TCP)				

CVE ID(s):
[CVE-2002-20001](#) 

Impacted software:

Summary:

The remote SSL/TLS server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange algorithms and thus could be prone to a denial of service (DoS) vulnerability.

Impact:

Insight:

The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE.

Detection:

Checks the supported cipher suites of the remote SSL/TLS server.

Solution:



- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered.

- Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For Postfix this limit can be configured via 'smtpd_client_new_tls_session_rate_limit' option, for other products please refer to the manual of the product in question on configuration possibilities.

Exploits:

Ransomware:

References:

<https://github.com/Balasy/dheater>  , https://www.researchgate.net/profile/Anton-Stiglic/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol 

Result:

'DHE' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA

'DHE' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA

'DHE' cipher suites accepted by this service via the TLSv1.2 protocol:... (showing first 500 characters)

Medium

OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)

New

HID:	HID-2-1-341234	First detected:	2022-10-13	Ticket:	Create ticket
CVSS v2 base:	4.3	Last detected:	2022-10-13	Published:	2021-11-16
CVSS v3.1 base:	5.3	Times detected:	1	Service modified:	2021-11-16
Operating system:	unknown				
Port:	22 (TCP)				

CVE ID(s):
[CVE-2016-20012](#)

Impacted software:
All currently OpenSSH versions are known to be affected.

Summary:
OpenBSD OpenSSH is prone to an information disclosure vulnerability.

Impact:

Insight:
OpenSSH allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session.

Detection:
Checks if a vulnerable version is present on the target host.

Solution:
No known solution is available as of 16th November, 2021.
Information regarding this issue will be updated once solution details are available.

Note: This issue is not treated as a security issue by the vendor so no update might be provided in the future.

Exploits:

Ransomware:

References:
<https://utcc.utoronto.ca/~cks/space/blog/tech/SSHKeysAreInfoLeak> , <https://rushter.com/blog/public-ssh-keys/> , <https://github.com/openssh/openssh-portable/pull/270>

Result:
Installed version: 9.9.99p1
Fixed version: None
Installation
path / port: 22/tcp

Legend and explanations

* The Open status is the sum of all vulnerabilities with the New and Active statuses.

Severity levels

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base group represents the intrinsic qualities of a vulnerability, the Temporal group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment. The Base metrics produce a score ranging from 0.0 to 10.0, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.

The CVSS Score is translated into a severity level in Holm Security VMP to simplify the vulnerability levels.

Translation from CVSS Score to Holm Security severity levels:

Severity level:	Info	Low	Medium	High	Critical
CVSS v2.0 score:	0	0,1–2,0	2,1–5,0	5,1–8,0	8,1–10
CVSS v3.x score:	0	0,1–2,0	2,1–5,0	5,1–8,0	8,1–10

Business risk

Business risk is calculated based on the severity of the vulnerability in relation to the business impact set on the asset or a related tag.

Read more in our knowledgebase:

<https://support.holmsecurty.com/hc/en-us/articles/115001910085-How-is-the-overall-business-risk-calculated->