Scan Report

March 22, 2021

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Win7". The scan started at Mon Mar 22 07:32:57 2021 UTC and ended at Mon Mar 22 08:03:59 2021 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
192.168.1.101	3	4	1	0	0
Total: 1	3	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 8 results selected by the filtering described above. Before filtering there were 38 results.

2 Results per Host

2.1 192.168.1.101

Host scan start	Mon Mar 22 07:34:03 2021 UTC
Host scan end	Mon Mar 22 08:03:54 2021 UTC

Service (Port)	Threat Level
80/tcp	High
445/tcp	High
135/tcp	Medium
80/tcp	Medium
21/tcp	Medium
general/tcp	Low

2.1.1 High 80/tcp

High (CVSS: 10.0)
NVT: MS15-034 HTTP.sys Remote Code Execution Vulnerability (Active Check)

Product detection result
`cpe:/a:microsoft:internet_information_services:7.5`
`Detected by Microsoft Internet Information Services (IIS) Detection (HTTP) (OID:`

... continues on next page ...

... continued from previous page ...

↪ 1.3.6.1.4.1.25623.1.0.900710)

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-034.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.

Solution
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior

Vulnerability Insight
Flaw exists due to the HTTP protocol stack 'HTTP.sys' that is triggered when parsing HTTP requests.

Vulnerability Detection Method
Send a special crafted HTTP GET request and check the response
Details: MS15-034 HTTP.sys Remote Code Execution Vulnerability (Active Check)
OID:1.3.6.1.4.1.25623.1.0.105257
Version used: 2020-11-25T11:26:55Z

Product Detection Result
Product: cpe:/a:microsoft:internet_information_services:7.5
Method: Microsoft Internet Information Services (IIS) Detection (HTTP)
OID: 1.3.6.1.4.1.25623.1.0.900710)

References
cve: CVE-2015-1635
url: https://support.microsoft.com/kb/3042553
url: https://technet.microsoft.com/library/security/MS15-034
url: http://pastebin.com/ypURDPc4
cert-bund: CB-K15/0527

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-0545

[return to 192.168.1.101]

2.1.2 High 445/tcp

High (CVSS: 9.3)
NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

Solution
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012 R2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows Server 2008 x32/x64 Service Pack 2

Vulnerability Insight
Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

Vulnerability Detection Method
Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.
Details: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)
OID:1.3.6.1.4.1.25623.1.0.810676
Version used: 2020-06-04T12:11:49Z

References

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2017-0143
cve: CVE-2017-0144
cve: CVE-2017-0145
cve: CVE-2017-0146
cve: CVE-2017-0147
cve: CVE-2017-0148
bid: 96703
bid: 96704
bid: 96705
bid: 96707
bid: 96709
bid: 96706
url: https://support.microsoft.com/en-in/kb/4013078
url: https://technet.microsoft.com/library/security/MS17-010
url: https://github.com/rapid7/metasploit-framework/pull/8167/files
cert-bund: CB-K17/0435
dfn-cert: DFN-CERT-2017-0448
```

High (CVSS: 9.0)
NVT: SMB Brute Force Logins With Default Credentials

Summary
A number of known default credentials are tried for the login via the SMB protocol.

Vulnerability Detection Result
`It was possible to login with the following credentials via the SMB protocol to ↪the 'IPC$' share. <User>:<Password>`
`administrator:admin123`

Solution
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Detection Method
Tries to login with a number of known default credentials via the SMB protocol.
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `2019-09-07T15:01:50Z`

[return to 192.168.1.101]

2.1.3 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: 49152/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.101[49152]
Port: 49153/tcp
     UUID: 06bba54a-be05-49f9-b0a0-30f790261023, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.101[49153]
     Annotation: Security Center
     UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.101[49153]
     Annotation: NRP server endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.101[49153]
     Annotation: DHCP Client LRPC Endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.101[49153]
     Annotation: DHCPv6 Client LRPC Endpoint
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.101[49153]
     Annotation: Event log TCPIP
Port: 49154/tcp
     UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.101[49154]
     Annotation: IP Transition Configuration endpoint
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.101[49154]
     UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.101[49154]
     Annotation: XactSrv service
     UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.101[49154]
     Annotation: IKE/Authip API
Port: 49155/tcp
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:192.168.1.101[49155]
Port: 49156/tcp
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.101[49156]
```

... continues on next page ...

... continued from previous page ...

```
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : SAM access
Port: 49157/tcp
      UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.101[49157]
      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:192.168.1.101[49157]
      Annotation: Remote Fw APIs
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: 2017-06-13T07:06:12Z

[return to 192.168.1.101]

2.1.4 Medium 80/tcp

Medium (CVSS: 5.0)
NVT: Microsoft IIS Default Welcome Page Information Disclosure Vulnerability

Product detection result

```
cpe:/a:microsoft:internet_information_services:7.5
Detected by Microsoft Internet Information Services (IIS) Detection (HTTP) (OID:
↪ 1.3.6.1.4.1.25623.1.0.900710)
```

Summary
The host is running Microsoft IIS Webserver and is prone to information disclosure vulnerability.

Vulnerability Detection Result

... continues on next page ...

... continued from previous page ...

Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to obtain sensitive information that could aid in further attacks.

Solution
Solution type: Mitigation
Disable the default pages within the server configuration.

Affected Software/OS
Microsoft Internet Information Services.

Vulnerability Insight
The flaw is due to misconfiguration of IIS Server, which allows to access default pages when the server is not used.

Vulnerability Detection Method
Details: `Microsoft IIS Default Welcome Page Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.802806
Version used: `2020-11-25T11:26:55Z`

Product Detection Result
Product: `cpe:/a:microsoft:internet_information_services:7.5`
Method: `Microsoft Internet Information Services (IIS) Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.900710)

[return to 192.168.1.101]

2.1.5 Medium 21/tcp

Medium (CVSS: 6.4)
NVT: Anonymous FTP Login Reporting

Summary
Reports if the remote FTP Server allows anonymous logins.

Vulnerability Detection Result
```
It was possible to login to the remote FTP service with the following anonymous
↪account(s):
anonymous:anonymous@example.com
ftp:anonymous@example.com
```

Impact
Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to:

... continues on next page ...

... continued from previous page ...

- gain access to sensitive files
- upload or delete files.

Solution
Solution type: Mitigation
If you do not want to share files, you should disable anonymous logins.

Vulnerability Insight
A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data.

Vulnerability Detection Method
Details: `Anonymous FTP Login Reporting`
OID:1.3.6.1.4.1.25623.1.0.900600
Version used: `2020-08-24T08:40:10Z`

References
`url: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497`

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

Summary
The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Vulnerability Detection Result
```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Non-anonymous sessions: 331 Password required for openvasvt.
Anonymous sessions:     331 Anonymous access allowed, send identity (e-mail name
↪) as password.
```

Impact
An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution
Solution type: Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.
Details: `FTP Unencrypted Cleartext Login`
OID:1.3.6.1.4.1.25623.1.0.108528
Version used: `2020-08-24T08:40:10Z`

[return to 192.168.1.101]

2.1.6 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

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

Vulnerability Detection 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: 523487
Packet 2: 523595
```

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

Solution
Solution type: Mitigation
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.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

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

Vulnerability Detection Method
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.

... continues on next page ...

... continued from previous page ...

Details: TCP timestamps
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: 2020-08-24T08:40:10Z

References
url: http://www.ietf.org/rfc/rfc1323.txt
url: http://www.ietf.org/rfc/rfc7323.txt
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152

[return to 192.168.1.101]