Scan Report

July 24, 2019

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 “Immediate scan of IP 172.16.1.100”. The scan started at Wed Jul 24 01:48:32 2019 UTC and ended at Wed Jul 24 01:54:12 2019 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
172.16.1.100	32	6	1	0	0
Total: 1	32	6	1	0	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
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.
It only lists hosts that produced issues.
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 39 results selected by the filtering described above. Before filtering there were 78 results.

2 Results per Host

2.1 172.16.1.100

Host scan start	Wed Jul 24 01:48:41 2019 UTC
Host scan end	Wed Jul 24 01:54:12 2019 UTC

Service (Port)	Threat Level
445/tcp	High
2222/tcp	High
general/tcp	High
1433/tcp	High
135/tcp	Medium
2222/tcp	Medium
general/tcp	Medium
3389/tcp	Medium
general/tcp	Low

2.1.1 High 445/tcp

High (CVSS: 10.0)
NVT: Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)

. . . continues on next page . . .

. . . continued from previous page . . .

Summary
This host is missing a critical security update according to Microsoft Bulletin MS10-012.

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

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or cause a denial of service or bypass the authentication mechanism via brute force technique.

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

Affected Software/OS
Microsoft Windows 7
Microsoft Windows 2000 Service Pack and prior
Microsoft Windows XP Service Pack 3 and prior
Microsoft Windows Vista Service Pack 2 and prior
Microsoft Windows Server 2003 Service Pack 2 and prior
Microsoft Windows Server 2008 Service Pack 2 and prior

Vulnerability Insight
- An input validation error exists while processing SMB requests and can be exploited to cause a buffer overflow via a specially crafted SMB packet.
- An error exists in the SMB implementation while parsing SMB packets during the Negotiate phase causing memory corruption via a specially crafted SMB packet.
- NULL pointer dereference error exists in SMB while verifying the 'share' and 'servername' fields in SMB packets causing denial of service.
- A lack of cryptographic entropy when the SMB server generates challenges during SMB NTLM authentication and can be exploited to bypass the authentication mechanism.

Vulnerability Detection Method
Details: `Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)`
OID:1.3.6.1.4.1.25623.1.0.902269
Version used: `2019-05-03T10:54:50+0000`

References
```
CVE: CVE-2010-0020, CVE-2010-0021, CVE-2010-0022, CVE-2010-0231
Other:
  URL:http://secunia.com/advisories/38510/
   URL:http://support.microsoft.com/kb/971468
   URL:http://www.vupen.com/english/advisories/2010/0345
   URL:http://www.microsoft.com/technet/security/bulletin/ms10-012.mspx
```

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 Edition Microsoft Windows Server 2012 Edition Microsoft Windows Server 2016 Microsoft Windows 8.1 x32/x64 Edition Microsoft Windows Server 2012 R2 Edition Microsoft Windows 7 x32/x64 Edition Service Pack 1 Microsoft Windows Vista x32/x64 Edition Service Pack 2 Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 Microsoft Windows Server 2008 x32/x64 Edition 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: `2019-05-03T10:54:50+0000`

References

```
CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147,
↪CVE-2017-0148
BID:96703, 96704, 96705, 96707, 96709, 96706
Other:
  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
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

Summary

A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
Admin:guest
```

Solution

Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Detection Method

Details: `SMB Brute Force Logins With Default Credentials`

OID:1.3.6.1.4.1.25623.1.0.804449

Version used: `$Revision: 13534 $`

High (CVSS: 9.0)

NVT: SMB Brute Force Logins With Default Credentials

Summary

A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
Guest:guest
```

Solution

Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Detection Method

Details: `SMB Brute Force Logins With Default Credentials`

OID:1.3.6.1.4.1.25623.1.0.804449

Version used: `$Revision: 13534 $`

High (CVSS: 9.0)

NVT: SMB Brute Force Logins With Default Credentials

Summary

A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪the 'IPC$' share. <User>:<Password>
User:guest
```

Solution

Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Detection Method

Details: `SMB Brute Force Logins With Default Credentials`

OID:1.3.6.1.4.1.25623.1.0.804449

Version used: `$Revision: 13534 $`

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

Summary

A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
User1:guest
```

Solution

Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Detection Method

Details: `SMB Brute Force Logins With Default Credentials`

OID:1.3.6.1.4.1.25623.1.0.804449

Version used: `$Revision: 13534 $`

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

Summary

A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
user-1:guest
```

Solution

Solution type: Mitigation

. . . continues on next page . . .

. . . continued from previous page . . .

Change the password as soon as possible.

Vulnerability Detection Method
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `$Revision: 13534 $`

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

Summary
A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
Test:guest
```

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

Vulnerability Detection Method
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `$Revision: 13534 $`

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

Summary
A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
root:guest
```

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

Vulnerability Detection Method
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449

. . . continues on next page . . .

. . . continued from previous page . . .

Version used: `$Revision: 13534 $`

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

Summary
A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
buh:guest
```

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

Vulnerability Detection Method
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `$Revision: 13534 $`

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

Summary
A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
boss:guest
```

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

Vulnerability Detection Method
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `$Revision: 13534 $`

. . . continues on next page . . .

. . . continued from previous page . . .

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

Summary
A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
ftp:guest
```

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

Vulnerability Detection Method
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `$Revision: 13534 $`

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

Summary
A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
rdp:guest
```

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

Vulnerability Detection Method
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `$Revision: 13534 $`

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

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
rdpuser:guest
```

Solution

Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Detection Method

Details: `SMB Brute Force Logins With Default Credentials`

OID:1.3.6.1.4.1.25623.1.0.804449

Version used: `$Revision: 13534 $`

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

Summary

A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
rdpadmin:guest
```

Solution

Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Detection Method

Details: `SMB Brute Force Logins With Default Credentials`

OID:1.3.6.1.4.1.25623.1.0.804449

Version used: `$Revision: 13534 $`

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

Summary

A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

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

. . . continues on next page . . .

. . . continued from previous page . . .

```
manager:guest
```

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

Vulnerability Detection Method
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `$Revision: 13534 $`

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

Summary
A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
support:guest
```

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

Vulnerability Detection Method
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `$Revision: 13534 $`

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

Summary
A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
work:guest
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `$Revision: 13534 $`

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

Summary
A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
netguest:guest
```

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

Vulnerability Detection Method
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `$Revision: 13534 $`

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

Summary
A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
superuser:guest
```

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

Vulnerability Detection Method
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `$Revision: 13534 $`

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

Summary
A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
ftpadmin:guest
```

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

Vulnerability Detection Method
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `$Revision: 13534 $`

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

Summary
A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
ftpuser:guest
```

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

Vulnerability Detection Method
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `$Revision: 13534 $`

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

Summary
A number of known default credentials is tried for log in via SMB protocol.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
operator:guest
```

Solution

Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Detection Method

Details: `SMB Brute Force Logins With Default Credentials`

OID:1.3.6.1.4.1.25623.1.0.804449

Version used: `$Revision: 13534 $`

High (CVSS: 9.0)

NVT: SMB Brute Force Logins With Default Credentials

Summary

A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
backup:guest
```

Solution

Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Detection Method

Details: `SMB Brute Force Logins With Default Credentials`

OID:1.3.6.1.4.1.25623.1.0.804449

Version used: `$Revision: 13534 $`

High (CVSS: 9.0)

NVT: SMB Brute Force Logins With Default Credentials

Summary

A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
asus:guest
```

. . . continues on next page . . .

. . . continued from previous page . . .

Solution

Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Detection Method

Details: `SMB Brute Force Logins With Default Credentials`

OID:1.3.6.1.4.1.25623.1.0.804449

Version used: `$Revision: 13534 $`

High (CVSS: 9.0)

NVT: SMB Brute Force Logins With Default Credentials

Summary

A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
nasadmin:guest
```

Solution

Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Detection Method

Details: `SMB Brute Force Logins With Default Credentials`

OID:1.3.6.1.4.1.25623.1.0.804449

Version used: `$Revision: 13534 $`

High (CVSS: 9.0)

NVT: SMB Brute Force Logins With Default Credentials

Summary

A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
nasuser:guest
```

Solution

Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Detection Method

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `$Revision: 13534 $`

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

Summary
A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
nas:guest
```

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

Vulnerability Detection Method
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `$Revision: 13534 $`

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

Summary
A number of known default credentials is tried for log in via SMB protocol.

Vulnerability Detection Result

```
It was possible to login with the following credentials via the SMB protocol to
↪the 'IPC$' share. <User>:<Password>
alex:guest
```

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

Vulnerability Detection Method
Details: `SMB Brute Force Logins With Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.804449
Version used: `$Revision: 13534 $`

[return to 172.16.1.100]

2.1.2 High 2222/tcp

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

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 (remote check)`
OID:1.3.6.1.4.1.25623.1.0.105257
Version used: `2019-05-03T12:31:27+0000`

References

```
CVE: CVE-2015-1635
Other:
  URL:https://support.microsoft.com/kb/3042553
   URL:https://technet.microsoft.com/library/security/MS15-034
   URL:http://pastebin.com/ypURDPc4
```

[return to 172.16.1.100]

2.1.3 High general/tcp

High (CVSS: 8.5)
NVT: Microsoft SQL Server Multiple Vulnerabilities (3065718) - Remote

Product detection result

```
cpe:/a:microsoft:sql_server:10.50.4000.0
Detected by Microsoft SQL TCP/IP listener is running (OID: 1.3.6.1.4.1.25623.1.0
↪.10144)
```

Summary

This host is missing an important security update according to Microsoft Bulletin MS15-058.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact

Successful exploitation will allow remote attackers to elevate the privileges or execute arbitrary code remotely.

Solution

Solution type: VendorFix

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

Affected Software/OS

Microsoft SQL Server 2008 for x86/x64 Edition Service Pack 3,
Microsoft SQL Server 2008 for x86/x64 Edition Service Pack 4,
Microsoft SQL Server 2008 R2 for x86/x64 Edition Service Pack 2,
Microsoft SQL Server 2008 R2 for x86/x64 Edition Service Pack 3,
Microsoft SQL Server 2012 for x86/x64 Edition Service Pack 1,
Microsoft SQL Server 2012 for x86/x64 Edition Service Pack 2,
Microsoft SQL Server 2014 for x86/x64 Edition.

Vulnerability Insight

Flaws exist due to,
- An improperly casts pointers to an incorrect class.
- An incorrectly handling internal function calls to uninitialized memory.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.
Details: `Microsoft SQL Server Multiple Vulnerabilities (3065718) - Remote`
OID:1.3.6.1.4.1.25623.1.0.805815
Version used: `2019-05-03T10:54:50+0000`

Product Detection Result

Product: `cpe:/a:microsoft:sql_server:10.50.4000.0`
Method: `Microsoft SQL TCP/IP listener is running`
OID: 1.3.6.1.4.1.25623.1.0.10144)

. . . continues on next page . . .

. . . continued from previous page . . .

References
```
CVE: CVE-2015-1761, CVE-2015-1762, CVE-2015-1763
Other:
  URL:https://support.microsoft.com/en-us/kb/3065718
   URL:https://technet.microsoft.com/library/security/MS15-058
```

[return to 172.16.1.100]

2.1.4 High 1433/tcp

High (CVSS: 10.0)
NVT: Microsoft SQL Server End Of Life Detection

Product detection result
```
cpe:/a:microsoft:sql_server:10.50.4000.0
Detected by Microsoft SQL TCP/IP listener is running (OID: 1.3.6.1.4.1.25623.1.0
↪.10144)
```

Summary
The Microsoft SQL Server version on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result
```
The "Microsoft SQL Server 2008 R2" version on the remote host has reached the en
↪d of life.
CPE:               cpe:/a:microsoft:sql_server:10.50.4000.0
Installed version: 10.50.4000.0
EOL version:       10.50
EOL date:          2019-07-09
```

Impact
An end of life version of Microsoft SQL Server 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.

Solution
Solution type: VendorFix
Update the Microsoft SQL Server version on the remote host to a still supported version.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft SQL Server End Of Life Detection`
OID:1.3.6.1.4.1.25623.1.0.108188
Version used: `$Revision: 11863 $`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result

```
Product: cpe:/a:microsoft:sql_server:10.50.4000.0
Method: Microsoft SQL TCP/IP listener is running
OID: 1.3.6.1.4.1.25623.1.0.10144)
```

References

```
Other:
  URL:https://support.microsoft.com/en-us/lifecycle/search?sort=PN&alpha=sql%20s
↪erver&Filter=FilterNO
   URL:https://en.wikipedia.org/wiki/History_of_Microsoft_SQL_Server#Release_sum
↪mary
```

[return to 172.16.1.100]

2.1.5 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:172.16.1.100[49152]
Port: 49153/tcp
     UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.100[49153]
     Annotation: NRP server endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.100[49153]
     Annotation: DHCP Client LRPC Endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.100[49153]
     Annotation: DHCPv6 Client LRPC Endpoint
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.100[49153]
     Annotation: Event log TCPIP
Port: 49154/tcp
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
     UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.100[49154]
     UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.100[49154]
     Annotation: IP Transition Configuration endpoint
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.100[49154]
     UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.100[49154]
     Annotation: XactSrv service
     UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.100[49154]
     Annotation: IKE/Authip API
     UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.100[49154]
     Annotation: Impl friendly name
Port: 49155/tcp
     UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.100[49155]
     Named pipe : lsass
     Win32 service or process : Netlogon
     Description : Net Logon service
     UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
     Endpoint: ncacn_ip_tcp:172.16.1.100[49155]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : LSA access
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.100[49155]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
     UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
     Endpoint: ncacn_ip_tcp:172.16.1.100[49155]
     Annotation: MS NT Directory DRS Interface
Port: 49157/tcp
     UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
     Endpoint: ncacn_http:172.16.1.100[49157]
     Named pipe : lsass
     Win32 service or process : Netlogon
     Description : Net Logon service
     UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
     Endpoint: ncacn_http:172.16.1.100[49157]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : LSA access
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
     Endpoint: ncacn_http:172.16.1.100[49157]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
     UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
     Endpoint: ncacn_http:172.16.1.100[49157]
     Annotation: MS NT Directory DRS Interface
Port: 49158/tcp
     UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.100[49158]
     Named pipe : lsass
     Win32 service or process : Netlogon
     Description : Net Logon service
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.100[49158]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
Port: 49161/tcp
     UUID: a00c021c-2be2-11d2-b678-0000f87a8f8e, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.100[49161]
     Annotation: PERFMON SERVICE
     UUID: d049b186-814f-11d1-9a3c-00c04fc9b232, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.100[49161]
     Annotation: NtFrs API
     UUID: f5cc59b4-4264-101a-8c59-08002b2f8426, version 1
     Endpoint: ncacn_ip_tcp:172.16.1.100[49161]
     Annotation: NtFrs Service
Port: 49168/tcp
     UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5
     Endpoint: ncacn_ip_tcp:172.16.1.100[49168]
     Named pipe : dnsserver
     Win32 service or process : dns.exe
     Description : DNS Server
Port: 49176/tcp
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:172.16.1.100[49176]
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.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method
Details: `DCE/RPC and MSRPC Services Enumeration Reporting`
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: `$Revision: 6319 $`

[return to 172.16.1.100]

2.1.6 Medium 2222/tcp

Medium (CVSS: 5.0)
NVT: Microsoft ASP.NET Information Disclosure Vulnerability (2418042)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS10-070.

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

Impact
Successful exploitation could allow remote attackers to decrypt and gain access to potentially sensitive data encrypted by the server or read data from arbitrary files within an ASP.NET application. Obtained information may aid in further attacks.

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

Affected Software/OS
Microsoft ASP.NET 1.0 Microsoft ASP.NET 4.0 Microsoft ASP.NET 3.5.1 Microsoft ASP.NET 1.1 SP1 and prior Microsoft ASP.NET 2.0 SP2 and prior Microsoft ASP.NET 3.5 SP1 and prior

Vulnerability Insight
The flaw is due to an error within ASP.NET in the handling of cryptographic padding when using encryption in CBC mode. This can be exploited to decrypt data via returned error codes from an affected server.

Vulnerability Detection Method
Details: `Microsoft ASP.NET Information Disclosure Vulnerability (2418042)`
OID:1.3.6.1.4.1.25623.1.0.901161
Version used: `2019-05-03T10:54:50+0000`

References
`CVE: CVE-2010-3332`
`BID:43316`
`Other:`

. . . continues on next page . . .

. . . continued from previous page . . .

```
  URL:http://www.vupen.com/english/advisories/2010/2429
   URL:http://www.microsoft.com/technet/security/bulletin/MS10-070.mspx
   URL:http://www.troyhunt.com/2010/09/fear-uncertainty-and-and-padding-oracle.h
↪tml
   URL:http://weblogs.asp.net/scottgu/archive/2010/09/18/important-asp-net-secur
↪ity-vulnerability.aspx
```

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result

```
The following input fields where identified (URL:input name):
http://172.16.1.100:2222/:pass
```

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `$Revision: 10726 $`

References

```
Other:
  URL:https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_S
↪ession_Management
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
URL:https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
URL:https://cwe.mitre.org/data/definitions/319.html
```

[return to 172.16.1.100]

2.1.7 Medium general/tcp

Medium (CVSS: 6.8)
NVT: Microsoft SQL Server Elevation of Privilege Vulnerability (2984340) - Remote

Product detection result

```
cpe:/a:microsoft:sql_server:10.50.4000.0
Detected by Microsoft SQL TCP/IP listener is running (OID: 1.3.6.1.4.1.25623.1.0
↪.10144)
```

Summary
This host is missing an important security update according to Microsoft Bulletin MS14-044.

Vulnerability Detection Result

```
The target host was found to be vulnerable
```

Impact
Successful exploitation will allow remote attackers to cause a Denial of Service or elevation of privilege.

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

Affected Software/OS
Microsoft SQL Server 2014 x64 Edition,
Microsoft SQL Server 2012 x86/x64 Edition Service Pack 1 and prior,
Microsoft SQL Server 2008 R2 x86/x64 Edition Service Pack 2 and prior,
Microsoft SQL Server 2008 x86/x64 Edition Service Pack 3 and prior.

Vulnerability Insight
Flaws are due to when,
- SQL Master Data Services (MDS) does not properly encode output.
- SQL Server processes an incorrectly formatted T-SQL query.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `Microsoft SQL Server Elevation of Privilege Vulnerability (2984340) - Remote`
OID:1.3.6.1.4.1.25623.1.0.805110
Version used: `2019-05-03T10:54:50+0000`

. . . continues on next page . . .

. . . continued from previous page . . .

Product Detection Result

Product: `cpe:/a:microsoft:sql_server:10.50.4000.0`
Method: `Microsoft SQL TCP/IP listener is running`
OID: 1.3.6.1.4.1.25623.1.0.10144)

References

```
CVE: CVE-2014-1820, CVE-2014-4061
BID:69071, 69088
Other:
  URL:https://technet.microsoft.com/library/security/MS14-044
```

[return to 172.16.1.100]

2.1.8 Medium 3389/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Report Weak Cipher Suites

Summary

This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Vulnerability Detection Result

```
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
```

Solution

Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

Vulnerability Insight

These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808).
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000).
- 1024 bit RSA authentication is considered to be insecure and therefore as weak.
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Details: `SSL/TLS: Report Weak Cipher Suites`
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: `$Revision: 11135 $`

References

```
CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000
Other:
  URL:https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-
↪1465_update_6.html
   URL:https://bettercrypto.org/
   URL:https://mozilla.github.io/server-side-tls/ssl-config-generator/
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary

The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Vulnerability Detection Result

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:                CN=SERVER.domain.local
Signature Algorithm:    sha1WithRSAEncryption
```

Solution

Solution type: Mitigation

Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight

The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)

Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1

. . . continues on next page . . .

. . . continued from previous page . . .

or
fingerprint1,Fingerprint2

Vulnerability Detection Method
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `$Revision: 11524 $`

References

```
Other:
  URL:https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with
↪-sha-1-based-signature-algorithms/
```

[return to 172.16.1.100]

2.1.9 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.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 68684
Packet 2: 68793
```

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/IPv4 implementations that implement RFC1323.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

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

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.

Details: `TCP timestamps`

OID:1.3.6.1.4.1.25623.1.0.80091

Version used: `$Revision: 14310 $`

References

```
Other:
  URL:http://www.ietf.org/rfc/rfc1323.txt
   URL:http://www.microsoft.com/en-us/download/details.aspx?id=9152
```

[return to 172.16.1.100]

This file was automatically generated.