Scan Report

November 21, 2018

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 www.moviescope.com”. The scan started at Wed Nov 21 19:54:05 2018 UTC and ended at Wed Nov 21 20:07:32 2018 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
172.43.35.10 www.moviescope.com	1	5	1	0	0
Total: 1	1	5	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 7 results selected by the filtering described above. Before filtering there were 42 results.

2 Results per Host

2.1 172.43.35.10

Host scan start	Wed Nov 21 19:54:31 2018 UTC
Host scan end	Wed Nov 21 20:07:31 2018 UTC

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

2.1.1 High 80/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.

. . . continues on next page . . .

. . . continued from previous page . . .

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
Run Windows Update and update the listed hotfixes or download and install the hotfixes from the referenced advisory.

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: `$Revision: 11872 $`

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 172.43.35.10]

2.1.2 Medium 80/tcp

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

Summary

. . . continues on next page . . .

. . . continued from previous page . . .

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://www.moviescope.com/:txtpwd
```

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
   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 172.43.35.10]

2.1.3 Medium 135/tcp

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

. . . continues on next page . . .

... continued from previous page ...

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: 2103/tcp
     UUID: 1088a980-eae5-11d0-8d9b-00a02453c337, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[2103]
     Annotation: Message Queuing - QM2QM V1
     UUID: 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[2103]
     Annotation: Message Queuing - RemoteRead V1
     UUID: 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[2103]
     Annotation: Message Queuing - QMRT V2
     UUID: fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[2103]
     Annotation: Message Queuing - QMRT V1
Port: 2105/tcp
     UUID: 1088a980-eae5-11d0-8d9b-00a02453c337, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[2105]
     Annotation: Message Queuing - QM2QM V1
     UUID: 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[2105]
     Annotation: Message Queuing - RemoteRead V1
     UUID: 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[2105]
     Annotation: Message Queuing - QMRT V2
     UUID: fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[2105]
     Annotation: Message Queuing - QMRT V1
Port: 2107/tcp
     UUID: 1088a980-eae5-11d0-8d9b-00a02453c337, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[2107]
     Annotation: Message Queuing - QM2QM V1
     UUID: 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[2107]
     Annotation: Message Queuing - RemoteRead V1
     UUID: 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[2107]
     Annotation: Message Queuing - QMRT V2
     UUID: fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[2107]
     Annotation: Message Queuing - QMRT V1
```

... continues on next page ...

. . . continued from previous page . . .

```
Port: 49152/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49152]
Port: 49153/tcp
     UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49153]
     Annotation: NRP server endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49153]
     Annotation: DHCP Client LRPC Endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49153]
     Annotation: DHCPv6 Client LRPC Endpoint
     UUID: abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49153]
     Annotation: Wcm Service
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49153]
     Annotation: Event log TCPIP
Port: 49154/tcp
     UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49154]
     Annotation: IdSegSrv service
     UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49154]
     Annotation: Proxy Manager provider server endpoint
     UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49154]
     UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49154]
     UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49154]
     Annotation: IP Transition Configuration endpoint
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49154]
     UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49154]
     Annotation: XactSrv service
     UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49154]
     Annotation: IKE/Authip API
     UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49154]
     Annotation: Proxy Manager client server endpoint
     UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49154]
     Annotation: Adh APIs
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
     UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49154]
     Annotation: Impl friendly name
Port: 49155/tcp
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49155]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:172.43.35.10[49155]
     Annotation: KeyIso
Port: 49156/tcp
     UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49156]
     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49156]
     Named pipe : spoolss
     Win32 service or process : spoolsv.exe
     Description : Spooler service
     UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49156]
     UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49156]
     UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49156]
Port: 49157/tcp
     UUID: 1088a980-eae5-11d0-8d9b-00a02453c337, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49157]
     Annotation: Message Queuing - QM2QM V1
     UUID: 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49157]
     Annotation: Message Queuing - RemoteRead V1
     UUID: 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49157]
     Annotation: Message Queuing - QMRT V2
     UUID: fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49157]
     Annotation: Message Queuing - QMRT V1
Port: 49215/tcp
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:172.43.35.10[49215]
Port: 49216/tcp
     UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
     Endpoint: ncacn_ip_tcp:172.43.35.10[49216]
     Annotation: Remote Fw APIs
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪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: `$Revision: 6319 $`

[return to 172.43.35.10]

2.1.4 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
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 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

. . . continues on next page . . .

. . . continued from previous page . . .

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

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=Server2016R2
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)

. . . continues on next page . . .

. . . continued from previous page . . .

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
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: 8810 $`

References

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

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary

The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result

```
Server Temporary Key Size: 1024 bits
```

Impact

An attacker might be able to decrypt the SSL/TLS communication offline.

Solution

Solution type: Workaround
Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. (see https://weakdh.org/sysadmin.html).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight

The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks the DHE temporary public key size.

```
Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.
↪..
```

OID:1.3.6.1.4.1.25623.1.0.106223

Version used: `$Revision: 11524 $`

References

```
Other:
  URL:https://weakdh.org/
   URL:https://weakdh.org/sysadmin.html
```

[return to 172.43.35.10]

2.1.5 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: 118649068
Packet 2: 118649175
```

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 also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

Affected Software/OS

TCP/IPv4 implementations that implement RFC1323.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

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: 10411 $`

References

```
Other:
  URL:http://www.ietf.org/rfc/rfc1323.txt
```

[return to 172.43.35.10]

This file was automatically generated.