YourIT!
Your Logo Goes Here

Security Assessment

External Vulnerability Scan Detail Report

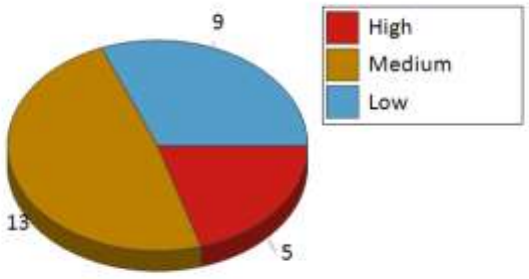
Scan Date: 3/12/2019

Prepared for:
Prospect Or Customer
Prepared by:
Your Company Name

3/12/2019

Table of Contents

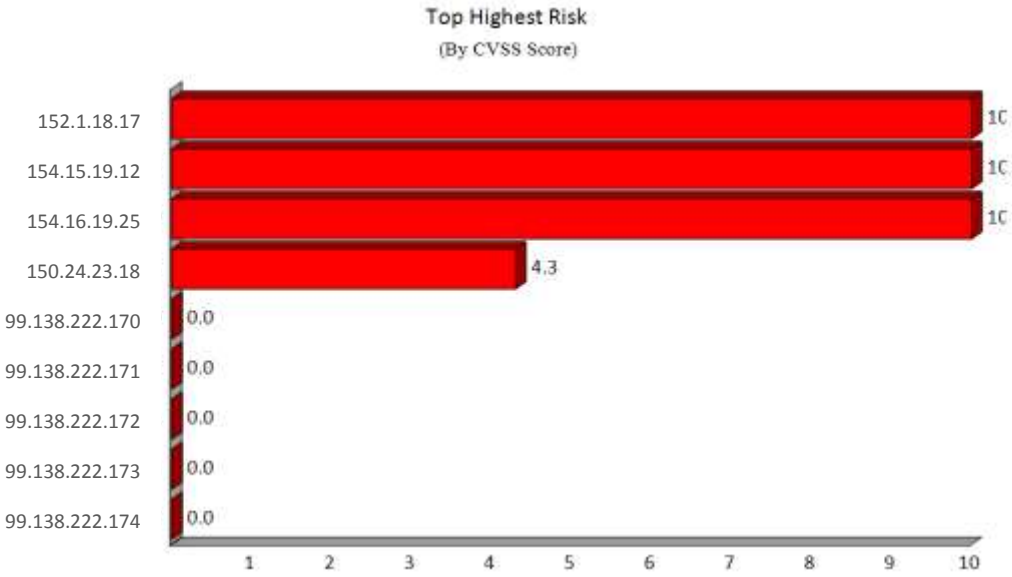
1 - Summary

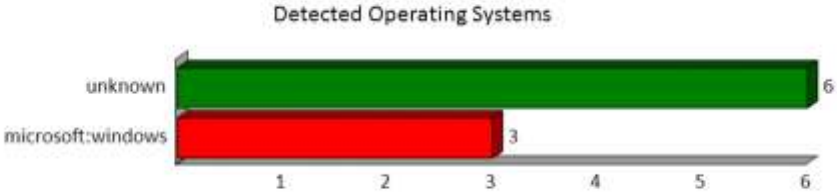


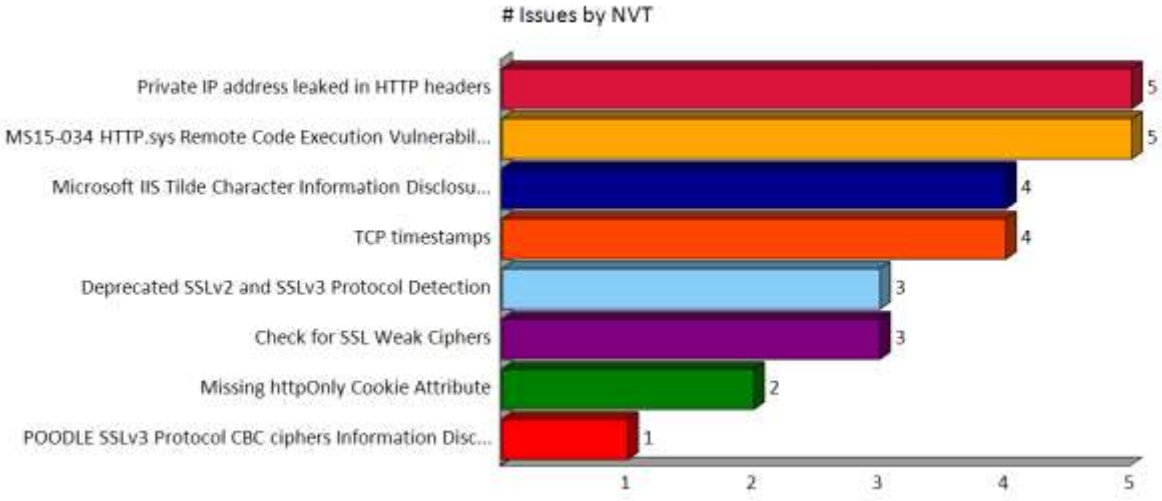
This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to mitigate these threats.

Host Issue Summary

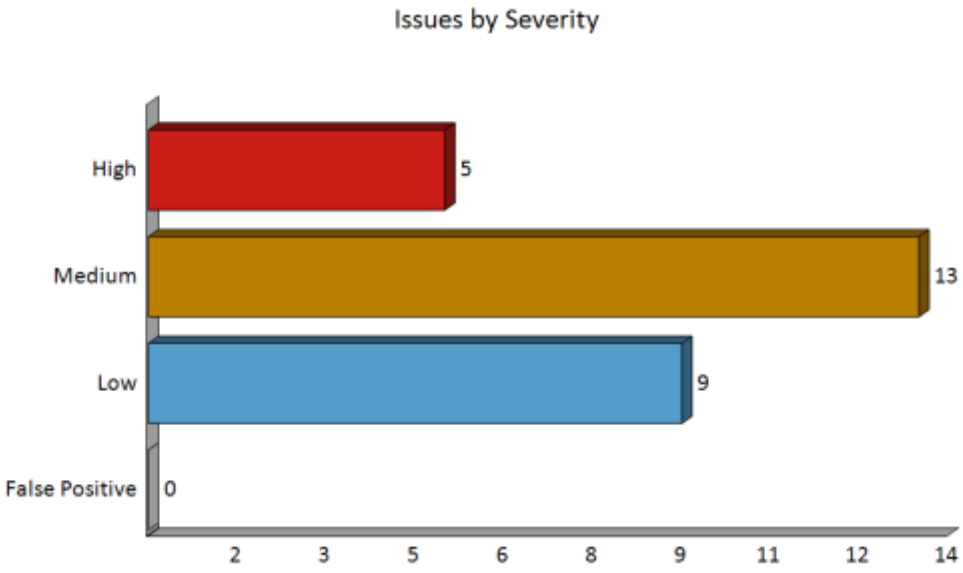
Host	Open Ports	High	Med	Low	False	Highest CVSS
150.24.23.18 (150-24-23-18 -static.hfc.comcastbusiness.net)	2	0	3	1	0	4.3
152.1.18.17 (ec2-152-1-18-17.gw-01.amazonaws.com)	2	**2**	5	3	0	10.0
154.15.19.12 (ec2-154-15-19-12.gw-01.amazonaws.com)	2	**2**	5	3	0	10.0
154.16.19.25 (ec2-154-16-19-25.gw-01.amazonaws.com)	2	**1**	0	2	0	10.0
99.138.222.170	0	0	0	0	0	0.0
99.138.222.171	0	0	0	0	0	0.0
99.138.222.172	0	0	0	0	0	0.0
99.138.222.173	0	0	0	0	0	0.0
99.138.222.174	0	0	0	0	0	0.0
Total: 9	8	**5**	**13**	9	0	10.0


Top Highest Risk
(By CVSS Score)
152.1.18.17
154.15.19.12
154.16.19.25
150.24.23.18
99.138.222.170
99.138.222.171
99.138.222.172
99.138.222.173
99.138.222.174
10
10
10
4.3
0.0
0.0
0.0
0.0
0.0
1
2
3
4
5
6
7
8
9
10

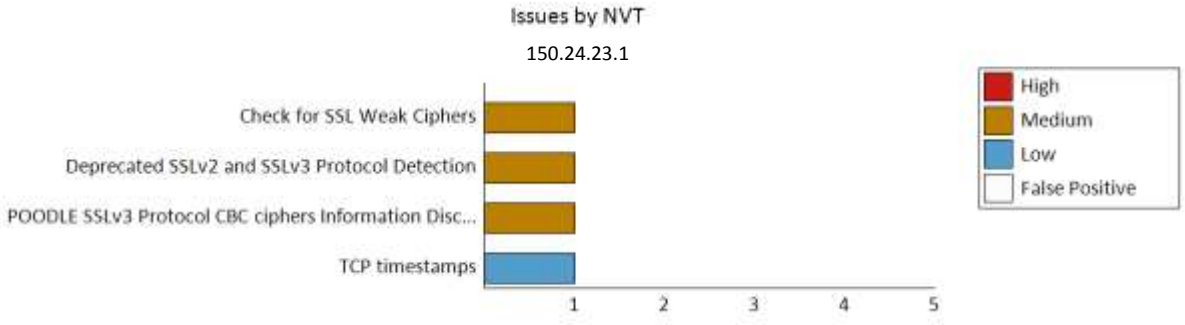

Detected Operating Systems
unknown
microsoft:windows
6
3
1
2
3
4
5
6


Issues by NVT
Private IP address leaked in HTTP headers
MS15-034 HTTP.sys Remote Code Execution Vulnerabil...
Microsoft IIS Tilde Character Information Disclosu...
TCP timestamps
Deprecated SSLv2 and SSLv3 Protocol Detection
Check for SSL Weak Ciphers
Missing httpOnly Cookie Attribute
POODLE SSLv3 Protocol CBC ciphers Information Disc...
5
5
4
4
3
3
2
1
1
2
3
4
5

2 - Scan Details



2.1 - 150.24.23.18 (150-24-23-18 -static.hfc.comcastbusiness.net)



Host Issue Summary

Host	Open Ports	High	Med	Low	False	Hightest CVSS
150.24.23.18 (150-24-23-18 -static.hfc.comcastbusiness.net)	2	0	3	1	0	4.3

Listening Ports

Port
443/tcp (https), 1723/tcp

NVT Issues Summary

NVT	Port	High	Med	Low	False	Highest CVSS
Check for SSL Weak Ciphers	443/tcp (https)	0	1	0	0	4.3
Deprecated SSLv2 and SSLv3 Protocol Detection	443/tcp (https)	0	1	0	0	4.3
POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability	443/tcp (https)	0	1	0	0	4.3
TCP timestamps		0	0	1	0	2.6

Security Issues

Medium (CVSS: 4.3) 443/tcp (https)
NVT: Check for SSL Weak Ciphers (OID: 1.3.6.1.4.1.25623.1.0.103440)

Summary

This routine search for weak SSL ciphers offered by a service.

Vulnerability Detection Result

Weak ciphers offered by this service: SSL3_RSA_RC4_128_MD5 SSL3_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA TLS1_RSA_RC4_128_MD5 TLS1_RSA_RC4_128_SHA

Solution

The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

Vulnerability Insight

These rules are applied for the evaluation of the cryptographic strength: - Any SSL/TLS using no cipher is considered weak. - All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol. - RC4 is considered to be weak. - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak. - 1024 bit RSA authentication is considered to be insecure and therefore as weak. - CBC ciphers in TLS < 1.2 are considered to be vulnerable to the BEAST or Lucky 13 attacks - 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: Check for SSL Weak Ciphers (OID: 1.3.6.1.4.1.25623.1.0.103440) Version used: $Revision: 2012 $

Medium (CVSS: 4.3) 443/tcp (https)
NVT: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012)

Summary

It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

Vulnerability Detection Result

In addition to TLSv1+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'Check SSL Weak Ciphers and Supported Ciphers' NVT.

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.

Solution

It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.

Vulnerability Insight

The SSLv2 and SSLv3 protocols containing known cryptographic flaws.

Vulnerability Detection Method

Check the used protocols of the services provided by this system. Details: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012) Version used: $Revision: 2699 $

References

https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report, https://bettercrypto.org/

Medium (CVSS: 4.3) 443/tcp (https)
NVT: POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.802087)

Summary

This host is installed with OpenSSL and is prone to information disclosure vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream. Impact Level: Application

Solution

Vendor released a patch to address this vulnerabiliy, For updates contact vendor or refer to https://www.openssl.org NOTE:

The only correct way to fix POODLE is to disable SSL v3.0

Vulnerability Insight

The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

Vulnerability Detection Method

Send a SSLv3 request and check the response. Details: POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.802087) Version used: $Revision: 2752 $

References

http://osvdb.com/113251, https://www.openssl.org/~bodo/ssl-poodle.pdf, https://www.imperialviolet.org/2014/10/14/poodle.html, https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html, http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html

Low (CVSS: 2.6)
NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

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: Paket 1: 202070569 Paket 2: 202070684

Impact

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

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

Vulnerability Insight

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

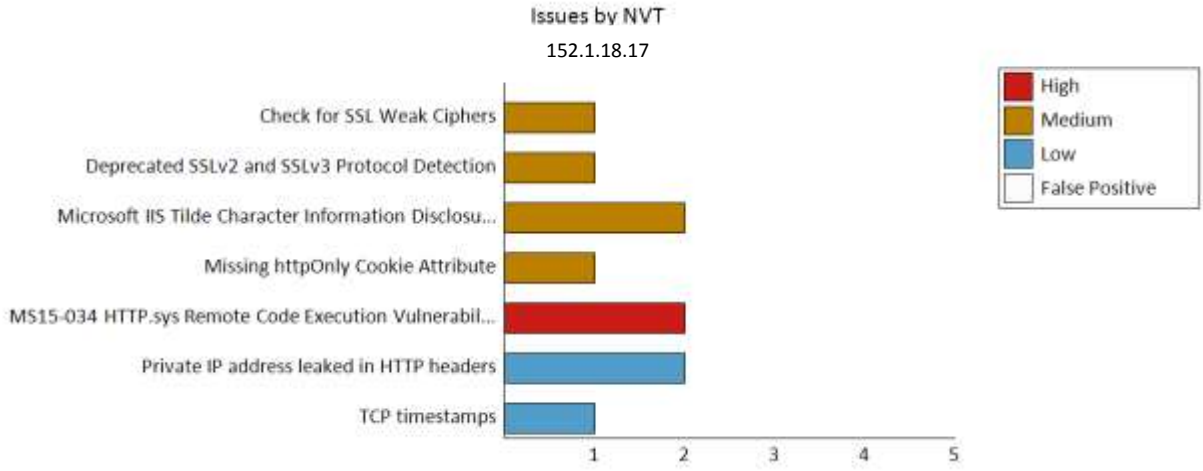
Vulnerability Detection Method

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: 787 $

References

http://www.ietf.org/rfc/rfc1323.txt

2.2 - 152.1.18.17 (ec2-152-1-18-17.gw-01.amazonaws.com)



Host Issue Summary

Host	Open Ports	High	Med	Low	False	Hightest CVSS
152.1.18.17 (ec2-152-1-18-17.gw-01.amazonaws.com)	2	**2**	5	3	0	10.0

Listening Ports

Port
80/tcp (http), 443/tcp (https)

NVT Issues Summary

NVT	Port	High	Med	Low	False	Highest CVSS
MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check)	80/tcp (http)	**1**	0	0	0	10.0
MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check)	443/tcp (https)	**1**	0	0	0	10.0
Missing httpOnly Cookie Attribute	80/tcp (http)	0	1	0	0	5.0
Microsoft IIS Tilde Character Information Disclosure Vulnerability	80/tcp (http)	0	1	0	0	5.0
Microsoft IIS Tilde Character Information Disclosure Vulnerability	443/tcp (https)	0	1	0	0	5.0
Check for SSL Weak Ciphers	443/tcp (https)	0	1	0	0	4.3
Deprecated SSLv2 and SSLv3 Protocol Detection	443/tcp (https)	0	1	0	0	4.3
TCP timestamps		0	0	1	0	2.6
Private IP address leaked in HTTP headers	80/tcp (http)	0	0	1	0	2.6
Private IP address leaked in HTTP headers	443/tcp (https)	0	0	1	0	2.6

Security Issues

High (CVSS: 10) 80/tcp (http)
NVT: MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check) (OID: 1.3.6.1.4.1.25623.1.0.105257)

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

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS15-034

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: 2646 $

References

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1635, https://support.microsoft.com/kb/3042553, https://technet.microsoft.com/library/security/MS15-034, http://pastebin.com/ypURDPc4

High (CVSS: 10) 443/tcp (https)
NVT: MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check) (OID: 1.3.6.1.4.1.25623.1.0.105257)

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

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS15-034

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: 2646 $

References

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1635, https://support.microsoft.com/kb/3042553,

https://technet.microsoft.com/library/security/MS15-034, http://pastebin.com/ypURDPc4

Medium (CVSS: 5)
NVT: Missing httpOnly Cookie Attribute (OID: 1.3.6.1.4.1.25623.1.0.105925)

Summary

The application is missing the 'httpOnly' cookie attribute

Vulnerability Detection Result

The cookies: Set-Cookie: AWSELB=918FD91B061BFBB96133DC6F3ED6599FF3354DA914A2B6FF71932FB2AE22FE331D6C11DE8CED9F45BA3735F86B18450B8A71DBE0A763 are missing the httpOnly attribute.

Impact

Application

Solution

Set the 'httpOnly' attribute for any session cookies.

Vulnerability Insight

The flaw is due to a cookie is not using the 'httpOnly' attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijack

Vulnerability Detection Method

Check all cookies sent by the application for a missing 'httpOnly' attribute Details: Missing httpOnly Cookie Attribute (OID: 1.3.6.1.4.1.25623.1.0.10

References

https://www.owasp.org/index.php/HttpOnly, https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-002)

Medium (CVSS: 5) 80/tcp (http)
NVT: Microsoft IIS Tilde Character Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.802887)

Summary

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

Vulnerability Detection Result

File/Folder name found on server starting with :500

Impact

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

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.

Vulnerability Insight

Microsoft IIS fails to validate a specially crafted GET request containing a '~' tilde character, which allows to disclose all short-names of folders and files having 4 letters extensions.

Vulnerability Detection Method

Details: Microsoft IIS Tilde Character Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.802887) Version used: $Revision: 2184 $

Product Detection Result

Product: cpe:/a:microsoft:iis:8.5 Method: Microsoft IIS Webserver Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900710)

References

http://www.osvdb.org/83771, http://www.exploit-db.com/exploits/19525, http://code.google.com/p/iis-shortname-scanner-poc, http://soroush.secproject.com/downloadable/iis_tilde_shortname_disclosure.txt, http://soroush.secproject.com/downloadable/microsoft_iis_tilde_character_vulnerability_feature.pdf

Medium (CVSS: 5) 443/tcp (https)
NVT: Microsoft IIS Tilde Character Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.802887)

Summary

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

Vulnerability Detection Result

File/Folder name found on server starting with :500

Impact

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

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.

Vulnerability Insight

Microsoft IIS fails to validate a specially crafted GET request containing a '~' tilde character, which allows to disclose all short-names of folders and files having 4 letters extensions.

Vulnerability Detection Method

Details: Microsoft IIS Tilde Character Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.802887) Version used: $Revision: 2184 $

Product Detection Result

Product: cpe:/a:microsoft:iis:8.5 Method: Microsoft IIS Webserver Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900710)

References

http://www.osvdb.org/83771, http://www.exploit-db.com/exploits/19525, http://code.google.com/p/iis-shortname-scanner-poc, http://soroush.secproject.com/downloadable/iis_tilde_shortname_disclosure.txt, http://soroush.secproject.com/downloadable/microsoft_iis_tilde_character_vulnerability_feature.pdf

Medium (CVSS: 4.3) 443/tcp (https)
NVT: Check for SSL Weak Ciphers (OID: 1.3.6.1.4.1.25623.1.0.103440)

Summary

This routine search for weak SSL ciphers offered by a service.

Vulnerability Detection Result

Weak ciphers offered by this service: SSL3_ECDHE_RSA_WITH_RC4_128_SHA SSL3_RSA_RC4_128_SHA TLS1_ECDHE_RSA_WITH_RC4_128_SHA TLS1_RSA_RC4_128_SHA TLS1_ECDHE_RSA_WITH_RC4_128_SHA TLS1_RSA_RC4_128_SHA TLS_1_2_RSA_WITH_RC4_128_SHA

Solution

The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

Vulnerability Insight

These rules are applied for the evaluation of the cryptographic strength: - Any SSL/TLS using no cipher is considered weak. - All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol. - RC4 is considered to be weak. - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak. - 1024 bit RSA authentication is considered to be insecure and therefore as weak. - CBC ciphers in TLS < 1.2 are considered to be vulnerable to the BEAST or Lucky 13 attacks - 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: Check for SSL Weak Ciphers (OID: 1.3.6.1.4.1.25623.1.0.103440) Version used: $Revision: 2012 $

Medium (CVSS: 4.3) 443/tcp (https)
NVT: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012)

Summary

It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

Vulnerability Detection Result

In addition to TLSv1+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'Check SSL Weak Ciphers and Supported Ciphers' NVT.

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.

Solution

It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.

Vulnerability Insight

The SSLv2 and SSLv3 protocols containing known cryptographic flaws.

Vulnerability Detection Method

Check the used protocols of the services provided by this system. Details: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012) Version used: $Revision: 2699 $

References

https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report, https://bettercrypto.org/

Low (CVSS: 2.6)
NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

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: Paket 1: 308067810 Paket 2: 308068105

Impact

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

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

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: 787 $

References

http://www.ietf.org/rfc/rfc1323.txt

Low (CVSS: 2.6) 80/tcp (http)
NVT: Private IP address leaked in HTTP headers (OID: 1.3.6.1.4.1.25623.1.0.10759)

Summary

This web server leaks a private IP address through its HTTP headers.

Vulnerability Detection Result

This web server leaks the following private IP address : 192.168.225.165

Impact

This may expose internal IP addresses that are usually hidden or masked behind a Network Address Translation (NAT) Firewall or proxy server.

Solution

See the references for possible workarounds and updates.

Vulnerability Insight

There is a known issue with IIS 4.0 doing this in its default configuration. Furthermore Microsoft Exchange CAS and OWA as well as other webservers or load balancers might be also affected.

Vulnerability Detection Method

Details: Private IP address leaked in HTTP headers (OID: 1.3.6.1.4.1.25623.1.0.10759) Version used: $Revision: 2411 $

References

https://support.microsoft.com/en-us/kb/218180, http://www.securityfocus.com/bid/1499/, http://foofus.net/?p=758

Low (CVSS: 2.6) 443/tcp (https)
NVT: Private IP address leaked in HTTP headers (OID: 1.3.6.1.4.1.25623.1.0.10759)

Summary

This web server leaks a private IP address through its HTTP headers.

Vulnerability Detection Result

This web server leaks the following private IP address : 192.168.225.165

Impact

This may expose internal IP addresses that are usually hidden or masked behind a Network Address Translation (NAT) Firewall or proxy server.

Solution

See the references for possible workarounds and updates.

Vulnerability Insight

There is a known issue with IIS 4.0 doing this in its default configuration. Furthermore Microsoft Exchange CAS and OWA as well as other webservers or load balancers might be also affected.

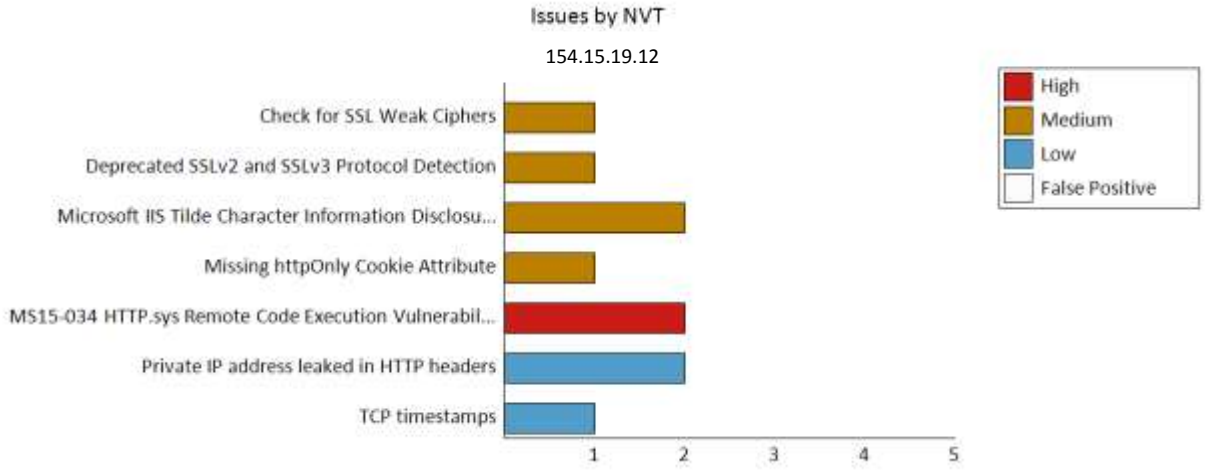
Vulnerability Detection Method

Details: Private IP address leaked in HTTP headers (OID: 1.3.6.1.4.1.25623.1.0.10759) Version used: $Revision: 2411 $

References

https://support.microsoft.com/en-us/kb/218180, http://www.securityfocus.com/bid/1499/, http://foofus.net/?p=758

2.3 - 154.15.19.12 (ec2-154-15-19-12.gw-01.amazonaws.com)



Host Issue Summary

Host	Open Ports	High	Med	Low	False	Hightest CVSS
154.15.19.12 (ec2-154-15-19-12.gw-01.amazonaws.com)	2	**2**	5	3	0	10.0

Listening Ports

Port
80/tcp (http), 443/tcp (https)

NVT Issues Summary

NVT	Port	High	Med	Low	False	Highest CVSS
MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check)	80/tcp (http)	**1**	0	0	0	10.0
MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check)	443/tcp (https)	**1**	0	0	0	10.0
Missing httpOnly Cookie Attribute	80/tcp (http)	0	1	0	0	5.0
Microsoft IIS Tilde Character Information Disclosure Vulnerability	80/tcp (http)	0	1	0	0	5.0
Microsoft IIS Tilde Character Information Disclosure Vulnerability	443/tcp (https)	0	1	0	0	5.0
Check for SSL Weak Ciphers	443/tcp (https)	0	1	0	0	4.3
Deprecated SSLv2 and SSLv3 Protocol Detection	443/tcp (https)	0	1	0	0	4.3
TCP timestamps		0	0	1	0	2.6
Private IP address leaked in HTTP headers	80/tcp (http)	0	0	1	0	2.6
Private IP address leaked in HTTP headers	443/tcp (https)	0	0	1	0	2.6

Security Issues

High (CVSS: 10)	80/tcp (http)

NVT: MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check) (OID: 1.3.6.1.4.1.25623.1.0.105257)

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

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS15-034

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: 2646 $

References

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1635, https://support.microsoft.com/kb/3042553, https://technet.microsoft.com/library/security/MS15-034, http://pastebin.com/ypURDPc4

High (CVSS: 10) 443/tcp (https)
NVT: MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check) (OID: 1.3.6.1.4.1.25623.1.0.105257)

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

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS15-034

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: 2646 $

References

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1635, https://support.microsoft.com/kb/3042553, https://technet.microsoft.com/library/security/MS15-034, http://pastebin.com/ypURDPc4

Medium (CVSS: 5)
NVT: Missing httpOnly Cookie Attribute (OID: 1.3.6.1.4.1.25623.1.0.105925)

Summary

The application is missing the 'httpOnly' cookie attribute

Vulnerability Detection Result

The cookies: Set-Cookie: AWSELB=49030F711E54F77F3D8567D69EA832FC7E9682DB5AE2D5E788FDD5A04B35259D6F5F262A6664B2E75D587AD40273B2AC59BC4707610D are missing the httpOnly attribute.

Impact

Application

Solution

Set the 'httpOnly' attribute for any session cookies.

Vulnerability Insight

The flaw is due to a cookie is not using the 'httpOnly' attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijack

Vulnerability Detection Method

Check all cookies sent by the application for a missing 'httpOnly' attribute Details: Missing httpOnly Cookie Attribute (OID: 1.3.6.1.4.1.25623.1.0.10

References

https://www.owasp.org/index.php/HttpOnly, https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-002)

Medium (CVSS: 5) 80/tcp (http)
NVT: Microsoft IIS Tilde Character Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.802887)

Summary

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

Vulnerability Detection Result

File/Folder name found on server starting with :apple

Impact

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

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.

Vulnerability Insight

Microsoft IIS fails to validate a specially crafted GET request containing a '~' tilde character, which allows to disclose all short-names of folders and files having 4 letters extensions.

Vulnerability Detection Method

Details: Microsoft IIS Tilde Character Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.802887) Version used: $Revision: 2184 $

Product Detection Result

Product: cpe:/a:microsoft:iis:8.5 Method: Microsoft IIS Webserver Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900710)

References

http://www.osvdb.org/83771, http://www.exploit-db.com/exploits/19525, http://code.google.com/p/iis-shortname-scanner-poc, http://soroush.secproject.com/downloadable/iis_tilde_shortname_disclosure.txt, http://soroush.secproject.com/downloadable/microsoft_iis_tilde_character_vulnerability_feature.pdf

Medium (CVSS: 5) 443/tcp (https)
NVT: Microsoft IIS Tilde Character Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.802887)

Summary

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

Vulnerability Detection Result

File/Folder name found on server starting with :apple

Impact

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

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.

Vulnerability Insight

Microsoft IIS fails to validate a specially crafted GET request containing a '~' tilde character, which allows to disclose all short-names of folders and files having 4 letters extensions.

Vulnerability Detection Method

Details: Microsoft IIS Tilde Character Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.802887) Version used: $Revision: 2184 $

Product Detection Result

Product: cpe:/a:microsoft:iis:8.5 Method: Microsoft IIS Webserver Version Detection (OID: 1.3.6.1.4.1.25623.1.0.900710)

References

http://www.osvdb.org/83771, http://www.exploit-db.com/exploits/19525, http://code.google.com/p/iis-shortname-scanner-poc, http://soroush.secproject.com/downloadable/iis_tilde_shortname_disclosure.txt, http://soroush.secproject.com/downloadable/microsoft_iis_tilde_character_vulnerability_feature.pdf

Medium (CVSS: 4.3) 443/tcp (https)
NVT: Check for SSL Weak Ciphers (OID: 1.3.6.1.4.1.25623.1.0.103440)

Summary

This routine search for weak SSL ciphers offered by a service.

Vulnerability Detection Result

Weak ciphers offered by this service: SSL3_ECDHE_RSA_WITH_RC4_128_SHA SSL3_RSA_RC4_128_SHA TLS1_ECDHE_RSA_WITH_RC4_128_SHA TLS1_RSA_RC4_128_SHA TLS1_ECDHE_RSA_WITH_RC4_128_SHA TLS1_RSA_RC4_128_SHA TLS_1_2_RSA_WITH_RC4_128_SHA

Solution

The configuration of this services should be changed so that it does not support the listed weak ciphers anymore.

Vulnerability Insight

These rules are applied for the evaluation of the cryptographic strength: - Any SSL/TLS using no cipher is considered weak. - All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol. - RC4 is considered to be weak. - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak. - 1024 bit RSA authentication is considered to be insecure and therefore as weak. - CBC ciphers in TLS < 1.2 are considered to be vulnerable to the BEAST or Lucky 13 attacks - 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: Check for SSL Weak Ciphers (OID: 1.3.6.1.4.1.25623.1.0.103440) Version used: $Revision: 2012 $

Medium (CVSS: 4.3) 443/tcp (https)
NVT: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012)

Summary

It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

Vulnerability Detection Result

In addition to TLSv1+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'Check SSL Weak Ciphers and Supported Ciphers' NVT.

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.

Solution

It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.

Vulnerability Insight

The SSLv2 and SSLv3 protocols containing known cryptographic flaws.

Vulnerability Detection Method

Check the used protocols of the services provided by this system. Details: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012) Version used: $Revision: 2699 $

References

https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report, https://bettercrypto.org/

Low (CVSS: 2.6)
NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

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: Paket 1: -269314483 Paket 2: -269314188

Impact

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

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

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: 787 $

References

http://www.ietf.org/rfc/rfc1323.txt

Low (CVSS: 2.6) 80/tcp (http)
NVT: Private IP address leaked in HTTP headers (OID: 1.3.6.1.4.1.25623.1.0.10759)

Summary

This web server leaks a private IP address through its HTTP headers.

Vulnerability Detection Result

This web server leaks the following private IP address : 192.168.226.191

Impact

This may expose internal IP addresses that are usually hidden or masked behind a Network Address Translation (NAT) Firewall or proxy server.

Solution

See the references for possible workarounds and updates.

Vulnerability Insight

There is a known issue with IIS 4.0 doing this in its default configuration. Furthermore Microsoft Exchange CAS and OWA as well as other webservers or load balancers might be also affected.

Vulnerability Detection Method

Details: Private IP address leaked in HTTP headers (OID: 1.3.6.1.4.1.25623.1.0.10759) Version used: $Revision: 2411 $

References

https://support.microsoft.com/en-us/kb/218180, http://www.securityfocus.com/bid/1499/, http://foofus.net/?p=758

Low (CVSS: 2.6) 443/tcp (https)
NVT: Private IP address leaked in HTTP headers (OID: 1.3.6.1.4.1.25623.1.0.10759)

Summary

This web server leaks a private IP address through its HTTP headers.

Vulnerability Detection Result

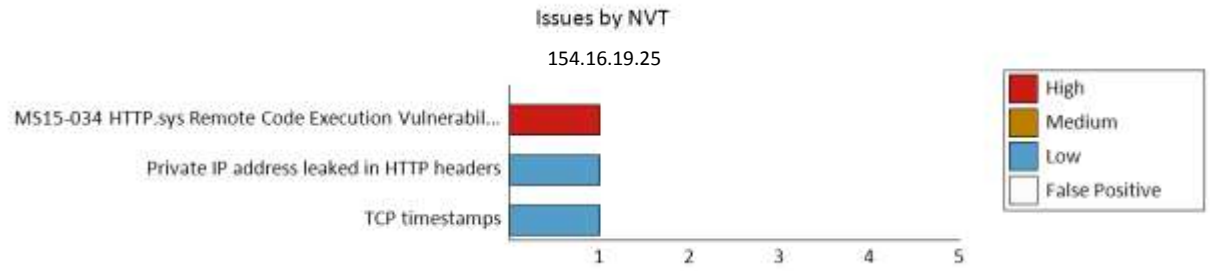
This web server leaks the following private IP address : 192.168.226.191

Impact

This may expose internal IP addresses that are usually hidden or masked behind a Network Address Translation (NAT) Firewall

or proxy server.
Solution See the references for possible workarounds and updates.
Vulnerability Insight There is a known issue with IIS 4.0 doing this in its default configuration. Furthermore Microsoft Exchange CAS and OWA as well as other webservers or load balancers might be also affected.
Vulnerability Detection Method Details: Private IP address leaked in HTTP headers (OID: 1.3.6.1.4.1.25623.1.0.10759) Version used: $Revision: 2411 $
References https://support.microsoft.com/en-us/kb/218180, http://www.securityfocus.com/bid/1499/, http://foofus.net/?p=758

2.4 - 154.16.19.25 (ec2-154-16-19-25.gw-01.amazonaws.com)



Host Issue Summary

Host	Open Ports	High	Med	Low	False	Hightest CVSS
154.16.19.25 (ec2-154-16-19-25.gw-01.amazonaws.com)	2	1	0	2	0	10.0

Listening Ports

Port
80/tcp (http), 443/tcp (https)

NVT Issues Summary

NVT	Port	High	Med	Low	False	Highest CVSS
MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check)	80/tcp (http)	1	0	0	0	10.0
TCP timestamps		0	0	1	0	2.6
Private IP address leaked in HTTP headers	80/tcp (http)	0	0	1	0	2.6

Security Issues

High (CVSS: 10) 80/tcp (http)
NVT: MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check) (OID: 1.3.6.1.4.1.25623.1.0.105257)

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

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, https://technet.microsoft.com/library/security/MS15-034

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: 2646 $

References

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1635, https://support.microsoft.com/kb/3042553, https://technet.microsoft.com/library/security/MS15-034, http://pastebin.com/ypURDPc4

Low (CVSS: 2.6)
NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

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: Paket 1: 1603581491 Paket 2: 1603581608

Impact

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

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

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: 787 $

References

http://www.ietf.org/rfc/rfc1323.txt

Low (CVSS: 2.6) 80/tcp (http)
NVT: Private IP address leaked in HTTP headers (OID: 1.3.6.1.4.1.25623.1.0.10759)

Summary

This web server leaks a private IP address through its HTTP headers.

Vulnerability Detection Result

This web server leaks the following private IP address : 192.168.226.85

Impact

This may expose internal IP addresses that are usually hidden or masked behind a Network Address Translation (NAT) Firewall or proxy server.

Solution See the references for possible workarounds and updates.
Vulnerability Insight There is a known issue with IIS 4.0 doing this in its default configuration. Furthermore Microsoft Exchange CAS and OWA as well as other webservers or load balancers might be also affected.
Vulnerability Detection Method Details: Private IP address leaked in HTTP headers (OID: 1.3.6.1.4.1.25623.1.0.10759) Version used: $Revision: 2411 $
References https://support.microsoft.com/en-us/kb/218180, http://www.securityfocus.com/bid/1499/, http://foofus.net/?p=758

2.5 - 99.138.222.170

Host Issue Summary

Host	Open Ports	High	Med	Low	False	Hightest CVSS
99.138.222.170	0	0	0	0	0	0.0

Listening Ports

None detected

NVT Issues Summary

None detected

Security Issues

None detected

2.6 - 99.138.222.171

Host Issue Summary

Host	Open Ports	High	Med	Low	False	Hightest CVSS
99.138.222.171	0	0	0	0	0	0.0

Listening Ports

None detected

NVT Issues Summary

None detected

Security Issues

None detected

2.7 - 99.138.222.172

Host Issue Summary

Host	Open Ports	High	Med	Low	False	Hightest CVSS
99.138.222.172	0	0	0	0	0	0.0

Listening Ports

None detected

NVT Issues Summary

None detected

Security Issues

None detected

2.8 - 99.138.222.173

Host Issue Summary

Host	Open Ports	High	Med	Low	False	Hightest CVSS
99.138.222.173	0	0	0	0	0	0.0

Listening Ports

None detected

NVT Issues Summary

None detected

Security Issues

None detected

2.9 - 99.138.222.174

Host Issue Summary

Host	Open Ports	High	Med	Low	False	Hightest CVSS
99.138.222.174	0	0	0	0	0	0.0

Listening Ports

None detected

NVT Issues Summary

None detected

Security Issues

None detected