Windows Server 2008 r2

Report generated by Nessus™ Mon, 06 Jul 2020 08:31:02 IST

TABLE OF CONTENTS

Vulnerabilities by Host

Remediations

Vulnerabilities by Host

192.168.1.216

CRITICAL	HIGH	MEDIUM	LOW	INFO
1	1	1	0	22

Scan Information

Start time: Mon Jul 6 08:18:10 2020

End time: Mon Jul 6 08:31:01 2020

Host Information

IP: 192.168.1.216

OS: Microsoft Windows Server 2003, Microsoft Windows Vista, Microsoft Windows Server 2008, Microsoft Windows 7, Microsoft Windows Server 2008 R2, Microsoft Windows Server 2012, Microsoft Windows 8, Microsoft Windows Server 2012 R2, Microsoft Windows 10, Microsoft Windows Server 2016, Microsoft Windows Server 2019

Vulnerabilities

51956 - MS11-004: Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution (2489256) (uncredentialed check)

Synopsis

The FTP service running on the remote host has a memory corruption vulnerability.

Description

The IIS FTP service running on the remote host has a heap-based buffer overflow vulnerability. The 'TELNET_STREAM_CONTEXT::OnSendData'

function fails to properly sanitize user input, resulting in a buffer overflow.

An unauthenticated, remote attacker can exploit this to execute arbitrary code.

See Also

https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2011/ms11-004

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 2008 R2, and 7.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

9.1 (CVSS:3.0/E:F/RL:O/RC:C)

CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID	45542
CVE	CVE-2010-3972
MSKB	2489256
XREF	EDB-ID:15803
XREF	MSFT:MS11-004

Exploitable With

Core Impact (true)

Plugin Information

Published: 2011/02/11, Modified: 2018/11/15

Plugin Output

tcp/21/ftp

105752 - Elasticsearch Transport Protocol Unspecified Remote Code Execution

Synopsis

Elasticsearch contains an unspecified flaw related to the transport protocol that may allow a remote attacker to execute arbitrary code.

Description

Elasticsearch could allow a remote attacker to execute arbitrary code on the system, caused by an error in the transport protocol. An attacker could exploit this vulnerability to execute arbitrary code on the system.

See Also

http://www.nessus.org/u?c6b6cf1a

Solution

Users should upgrade to 1.6.1 or 1.7.0. Alternately, ensure that only trusted applications have access to the transport protocol port

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2015-5377

Plugin Information

Published: 2018/01/11, Modified: 2019/11/08

Plugin Output

tcp/9200/elasticsearch

```
URL               : http://192.168.1.216:9200/
Installed version : 1.1.1
Fixed version     : 1.6.1
```

62940 - MS12-073: Vulnerabilities in Microsoft IIS Could Allow Information Disclosure (2733829) (uncredentialed check)

Synopsis

The Microsoft IIS service running on the remote system contains flaws that could lead to an unauthorized information disclosure.

Description

The FTP service in the version of Microsoft IIS 7.0 or 7.5 on the remote Windows host is affected by a command injection vulnerability that could result in unauthorized information disclosure.

See Also

https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2012/ms12-073

Solution

Microsoft has released a set of patches for Vista, 2008, 7, and 2008 R2.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

BID	56440

CVE	CVE-2012-2532
MSKB	2716513
MSKB	2719033
XREF	MSFT:MS12-073
XREF	IAVB:2012-B-0111

Plugin Information

Published: 2012/11/16, Modified: 2018/11/15

Plugin Output

tcp/21/ftp

21745 - Authentication Failure - Local Checks Not Run

Synopsis

The local security checks are disabled.

Description

Local security checks have been disabled for this host because either the credentials supplied in the scan policy did not allow Nessus to log into it or some other problem occurred.

Solution

Address the problem(s) so that local security checks are enabled.

Risk Factor

None

Plugin Information

Published: 2006/06/23, Modified: 2018/11/02

Plugin Output

tcp/0

```
The following service errors were logged :
  - It was not possible to log into the remote host via smb (unable to create a socket).
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/06/12

Plugin Output

tcp/21/ftp

```
Port 21/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/06/12

Plugin Output

tcp/22

```
Port 22/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/06/12

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/06/12

Plugin Output

tcp/1617

```
Port 1617/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/06/12

Plugin Output

tcp/4848/www

```
Port 4848/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/06/12

Plugin Output

tcp/5985/www

```
Port 5985/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/06/12

Plugin Output

tcp/8020/www

```
Port 8020/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/06/12

Plugin Output

tcp/8022/www

```
Port 8022/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/06/12

Plugin Output

tcp/8027

```
Port 8027/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/06/12

Plugin Output

tcp/8080/www

```
Port 8080/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/06/12

Plugin Output

tcp/8282/www

```
Port 8282/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/06/12

Plugin Output

tcp/8383/www

```
Port 8383/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/06/12

Plugin Output

tcp/8484/www

```
Port 8484/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/06/12

Plugin Output

tcp/8585/www

```
Port 8585/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/06/12

Plugin Output

tcp/9200/elasticsearch

```
Port 9200/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/06/12

Plugin Output

tcp/49153

```
Port 49153/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/06/12

Plugin Output

tcp/49154

```
Port 49154/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/06/12

Plugin Output

tcp/49171

```
Port 49171/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2020/06/12

Plugin Output

tcp/49173

```
Port 49173/tcp was found to be open
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- Whether credentialed or third-party patch management checks are possible.
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2020/06/12

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.10.0
Plugin feed version : 202007032004
Scanner edition used : Nessus Home
Scan type : Normal
Scan policy used : Test 2
Scanner IP : 192.168.1.100
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
```

```
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2020/7/6 8:18 IST
Scan duration : 671 sec
```

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2020/06/12

Plugin Output

tcp/0

```
. You need to take the following 2 actions :


[ Elasticsearch Transport Protocol Unspecified Remote Code Execution (105752) ]

+ Action to take : Users should upgrade to 1.6.1 or 1.7.0. Alternately, ensure that only trusted
 applications have access to the transport protocol port


[ MS12-073: Vulnerabilities in Microsoft IIS Could Allow Information Disclosure (2733829)
 (uncredentialed check) (62940) ]

+ Action to take : Microsoft has released a set of patches for Vista, 2008, 7, and 2008 R2.
```

Remediations

Suggested Remediations

Taking the following actions across 1 hosts would resolve 66% of the vulnerabilities on the network.

ACTION TO TAKE	VULNS	HOSTS
Elasticsearch Transport Protocol Unspecified Remote Code Execution: Users should upgrade to 1.6.1 or 1.7.0. Alternately, ensure that only trusted applications have access to the transport protocol port	1	1
MS12-073: Vulnerabilities in Microsoft IIS Could Allow Information Disclosure (2733829) (uncredentialed check): Microsoft has released a set of patches for Vista, 2008, 7, and 2008 R2.	1	1