

Nessus

Scansione di Meta

Scan Meta

[Back to My Scans](#)

ConfigureAudit TrailLaunchReportExport

Hosts1Vulnerabilities67Remediations3History1

FilterSearch Hosts1 Host

Host


Vulnerabilities

192.168.1.139107269132

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 7:07 AM
End: Today at 7:16 AM
Elapsed: 9 minutes

Vulnerabilities



Scan Meta

[Back to My Scans](#)

ConfigureAudit TrailLaunchReportExport

Hosts1Vulnerabilities67Remediations3History1

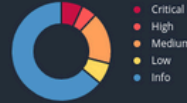
FilterSearch Vulnerabilities67 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	
CRITICAL	10.0 *	7.4	0.6988	UnrealIRCd Backdoor Detection	Backdoors	1	
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1	
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2	
CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1	
MIXED	Apache Tomcat (Multiple Issues)	Web Servers	4	
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	
HIGH	7.5	5.9	0.0358	Samba Badlock Vulnerability	General	1	
HIGH	7.5 *	5.9	0.015	rlogin Service Detection	Service detection	1	
HIGH	7.5 *	5.9	0.015	rsh Service Detection	Service detection	1	
HIGH	7.5			NFS Shares World Readable	RPC	1	
MIXED	SSL (Multiple Issues)	General	28	
MIXED	ISC Bind (Multiple Issues)	DNS	5	
MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2	
MEDIUM	6.5			Unencrypted Telnet Server	Misc.	1	
MEDIUM	5.9	4.4	0.9524	SSL DROWN Attack Vulnerability (Decrypting RSA with Obs...	Misc.	1	
MEDIUM	5.9	4.4	0.0031	SSL Anonymous Cipher Suites Supported	Service detection	1	
MIXED	DNS (Multiple Issues)	DNS	6	
MIXED	SSH (Multiple Issues)	Misc.	6	
MIXED	HTTP (Multiple Issues)	Web Servers	5	
MIXED	SMB (Multiple Issues)	Misc.	2	
MIXED	TLS (Multiple Issues)	Misc.	2	
MIXED	TLS (Multiple Issues)	SMTP problems	2	

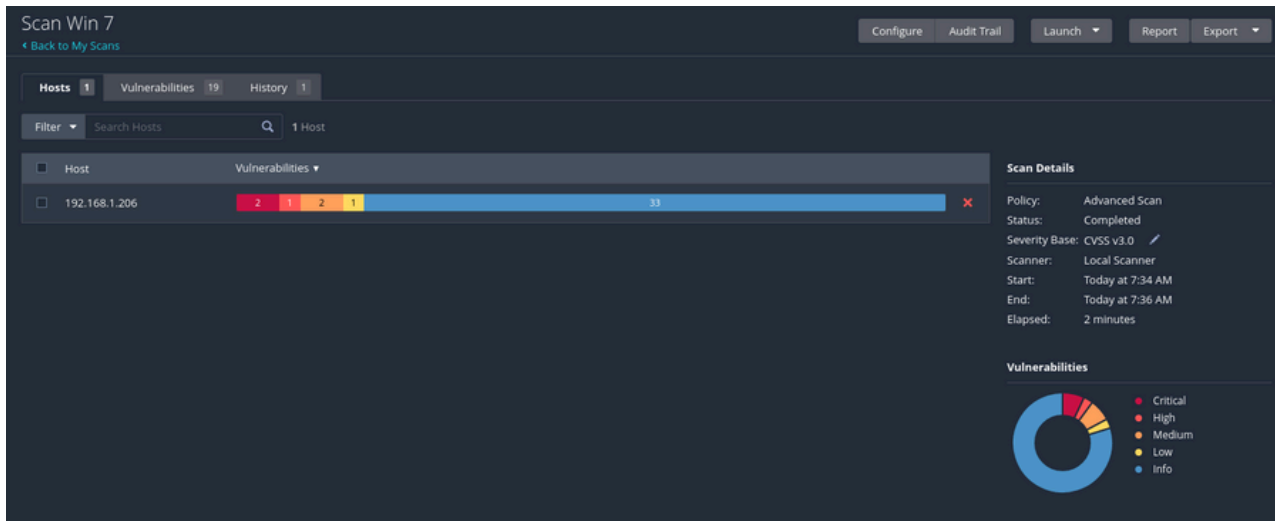
Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 7:07 AM
End: Today at 7:16 AM
Elapsed: 9 minutes

Vulnerabilities



Scansione di Win 7



Scan Win 7 / 192.168.1.206

← Back to Hosts

Configure Audit Trail Launch Report Export

Vulnerabilities 19

Filter Search Vulnerabilities 19 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count		
MIXED	Microsoft Windows (Multiple Issues)	Windows	5	⊙	✎
MIXED	SMB (Multiple Issues)	Misc.	2	⊙	✎
LOW	2.1 *	4.2	0.8808	ICMP Timestamp Request Remote Date Disclosure	General	1	⊙	✎
INFO	SMB (Multiple Issues)	Windows	7	⊙	✎
INFO	DCE Services Enumeration	Windows	8	⊙	✎
INFO	Nessus SYN scanner	Port scanners	3	⊙	✎
INFO	Common Platform Enumeration (CPE)	General	1	⊙	✎
INFO	Device Type	General	1	⊙	✎
INFO	Ethernet Card Manufacturer Detection	Misc.	1	⊙	✎
INFO	Ethernet MAC Addresses	General	1	⊙	✎
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1	⊙	✎
INFO	Link-Local Multicast Name Resolution (LLMNR) Detection	Service detection	1	⊙	✎
INFO	Nessus Scan Information	Settings	1	⊙	✎
INFO	Nessus Windows Scan Not Performed with Admin Privileges	Settings	1	⊙	✎
INFO	OS Identification	General	1	⊙	✎
INFO	OS Security Patch Assessment Not Available	Settings	1	⊙	✎
INFO	Target Credential Status by Authentication Protocol - No Cr...	Settings	1	⊙	✎
INFO	TCP/IP Timestamps Supported	General	1	⊙	✎
INFO	Traceroute Information	General	1	⊙	✎

Host Details

IP: 192.168.1.206
DNS: Dngste7.wind3.hub
MAC: 08:00:27:3F:F6:D5
OS: Microsoft Windows 7 Professional
Start: Today at 7:34 AM
End: Today at 7:36 AM
Elapsed: 2 minutes
KB: [Download](#)

Vulnerabilities

Donut chart showing vulnerability distribution: Critical (red), High (orange), Medium (yellow), Low (blue), Info (light blue).

Vulnerabilità Meta

Scan Meta / Plugin #46882

ConfigureAudit TrailLaunchReportExport

Hosts1Vulnerabilities67Remediations3History1

CRITICALUnrealIRCd Backdoor Detection

>Plugin Details

Description

The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

See Also

<https://seclists.org/fulldisclosure/2010/jun/277>
<https://seclists.org/fulldisclosure/2010/jun/284>
<http://www.unrealircd.com/txt/unrealircadvisory.20100612.txt>

Output

The remote IRC server is running as :

uid=0(root) gid=0(root)

To see debug logs, please visit individual host

PortHosts

6667/tcp/irc192.168.1.139

Severity: Critical

ID: 46882

Version: 1.16

Type: remote

Family: Backdoors

Published: June 14, 2010

Modified: April 11, 2022

VPR Key Drivers

Threat Recency: No recorded events

Threat Intensity: Very Low

Exploit Code Maturity: Functional

Age of Vuln: 730 days +

Product Coverage: Low

CVSSv3 Impact Score: 5.9

Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 7.4

Exploit Prediction Scoring System (EPSS): 0.6988

Risk Factor: Critical

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Temporal Score: 8.3

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS v2.0 Temporal Vector:

UnrealIRCd Backdoor: Questa vulnerabilità è critica perché consente a un attaccante di accedere senza autorizzazione al sistema informatico, ottenendo il controllo completo del sistema, senza dover superare le normali misure di sicurezza.

Scan Meta / Plugin #61708

ConfigureAudit TrailLaunchReportExport

Hosts1Vulnerabilities67Remediations3History1

CRITICALVNC Server 'password' Password

<>Plugin Details

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Output

Nessus logged in using a password of "password".

To see debug logs, please visit individual host

PortHosts

5900/tcp/vnc192.168.1.139

Severity: Critical

ID: 61708

Version: \$Revision: 1.2 \$

Type: remote

Family: Gain a shell remotely

Published: August 29, 2012

Modified: September 24, 2015

Risk Information

Risk Factor: Critical

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

Default Account: true

Exploited by Nessus: true

VNC Server Password: Questa vulnerabilità indica che il server VNC in esecuzione sull'host remoto è debole, e un attaccante non autorizzato potrebbe sfruttare questa debolezza per prendere il controllo del sistema.

Scan Meta / Plugin #20007

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

Hosts 1 Vulnerabilities 67 Remediations 3 History 1

CRITICAL

SSL Version 2 and 3 Protocol Detection

<

>

Plugin Details

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.

See Also

<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>
<http://www.nessus.org/u/7b06c7e95>
<http://www.nessus.org/u/7247c4540>
<https://www.openssl.org/~bodo/ssl-poodle.pdf>
<http://www.nessus.org/u/75d15ba70>
<https://www.imperialviolet.org/2014/10/14/poodle.html>
<https://tools.ietf.org/html/rfc7507>
<https://tools.ietf.org/html/rfc7568>

Output

```
- SSLv2 is enabled and the server supports at least one cipher.

Low Strength Ciphers (<= 64-bit key)

Name                Code                KEX                Auth                Encryption                MAC                export
-----
EXP-RC2-CBC-MD5      RBA(512)            RSA                RC2-CBC(40)          MD5                        export
EXP-RC4-MD5          RBA(512)            RSA                RC4(40)              MD5                        export

More...
```

To see debug logs, please visit individual host

Port	Hosts
25 / tcp / smtp	192.168.1.139

SSL Version 2 and 3 Protocol: Queste due versioni del protocollo SSL sono obsolete e presentano gravi vulnerabilità. Un attaccante che si trova nel mezzo (attacco Man-in-the-Middle) potrebbe intercettare e manipolare le comunicazioni tra il server e il client.

Scan Meta / Plugin #51988

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

Hosts 1 Vulnerabilities 67 Remediations 3 History 1

CRITICAL

Bind Shell Backdoor Detection

<

>

Plugin Details

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Output

```
Nessus was able to execute the command "id" using the following request :
```

```
This produced the following truncated output (limited to 10 lines) :
..... snip .....
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
..... snip .....
```

To see debug logs, please visit individual host

Port	Hosts
1524 / tcp / wild_shell	192.168.1.139

Bind Shell Backdoor: Questa vulnerabilità non richiede alcuna autenticazione. Un attaccante può sfruttarla per connettersi da remoto al sistema e inviare comandi, come ad esempio l'installazione di malware.

Scan Meta / Plugin #90509

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 67 Remediations 3 History 1

HIGH Samba Badlock Vulnerability

Description
The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

Solution
Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

See Also
<http://badlock.org>
<https://www.samba.org/samba/security/CVE-2016-2118.html>

Output
Nessus detected that the Samba Badlock patch has not been applied.

To see debug logs, please visit individual host

Port	Hosts
445 / tcp / cifs	192.168.1.139

Plugin Details

Severity: High
ID: 90509
Version: 1.8
Type: remote
Family: General
Published: April 13, 2016
Modified: November 20, 2019

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Medium
CVSSv3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 5.9
Exploit Prediction Scoring System (EPSS): 0.0358
Risk Factor: Medium

CVSS v3.0 Base Score: 7.5
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C
CVSS v3.0 Temporal Score: 6.5
CVSS v2.0 Base Score: 6.8
CVSS v2.0 Temporal Score: 5.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P
CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:O/RC:C

Vulnerability Information

CPE: cpe:/a:samba:samba
Exploit Available: false
Exploit Ease: No known exploits are available
Patch Pub Date: April 12, 2016
Vulnerability Pub Date: March 23, 2016
In the news: true

Samba Badlock: Con questa vulnerabilità, un attaccante può eseguire un attacco Man-in-the-Middle, intercettando il traffico tra client e server e forzando un downgrade dell'autenticazione, compromettendo la sicurezza della comunicazione.

Daniel_Gabriel_Costeanu