METASPLOITABLE

FINANCIAL EXECUTIVE AND TECNICAL REPORT

2024

BUILDING TOWARDS SUCCESS

www.exemple.com

TABLE OF CONTENTS

Vulnerabilities by Host

Executive Summary: Nessus Security Analysis

Scanning Objective:

The Nessus scan was conducted to evaluate the security of the computer system and identify potential vulnerabilities that could compromise the integrity, confidentiality and availability of data. Through the analysis, our focus was on identifying flaws in system configuration, know software vulnerabilities and other potential security threats.

Key Findings:

During the scan, several critical vulnerabilities were identified, including exposures to possibile external attacks, configuration defects that could facilitate unauthorizied access, and gaps in security patch management. Additionally, risks associated with weak access credential configurations and potential violations of security policy were detected.

Racommendations:

To mitigate the identified risks and improve the overall security of the system, it is recommended to adopt the following measures:

- Apply security patches to address indentified vulnerabilities.
- Review and strengthen security policies related to access credential management, including the implementation of multi-factor authentication.
- Conduct regular securitu scans and configuration checks to promptly identify new vulnerabilities and ensure the maintenance of a secure environment.
- Educate staff on the importance of cybersecurity practices and promote a culture of security awareness within the organization.

By adopting these recommendations, we are committed to enhacing the protection of you computers environment and mitigating the risks associated with the vulnerabilities identified during the Nessus scan.

Economic associated with vulnerability

To calculate the potential economic savings associated with each vulnerability and the total of the indicated vulnerabilities, we can consider several factors, including:

- The average time required to exploit the vulnerability.
- The average cost of an attack caused by exploiting the vulnerability.
- The number of systems affected by the vulnerabilities.
- The estimated time of repair each vulnerability.
- The estimated cost to fix each vulnerability.

Since this is an exercise I don't have specific information about systems, I will use hypothetical values to illustrate the calculation.

Calculation of a single vulnerability (e.g. Apache Tomcat SEoL <=5.5.X):

Let's assume:

- Avarage time to exploite the vulnerability: 30 days.
- Avarage cost of and attack: 50.000 euro.
- Number of systems affected: 10.
- Estimated time to repair the vulnerability: 7 days.
- Estimated cost to fix the vulnerability: 5.000 euro.

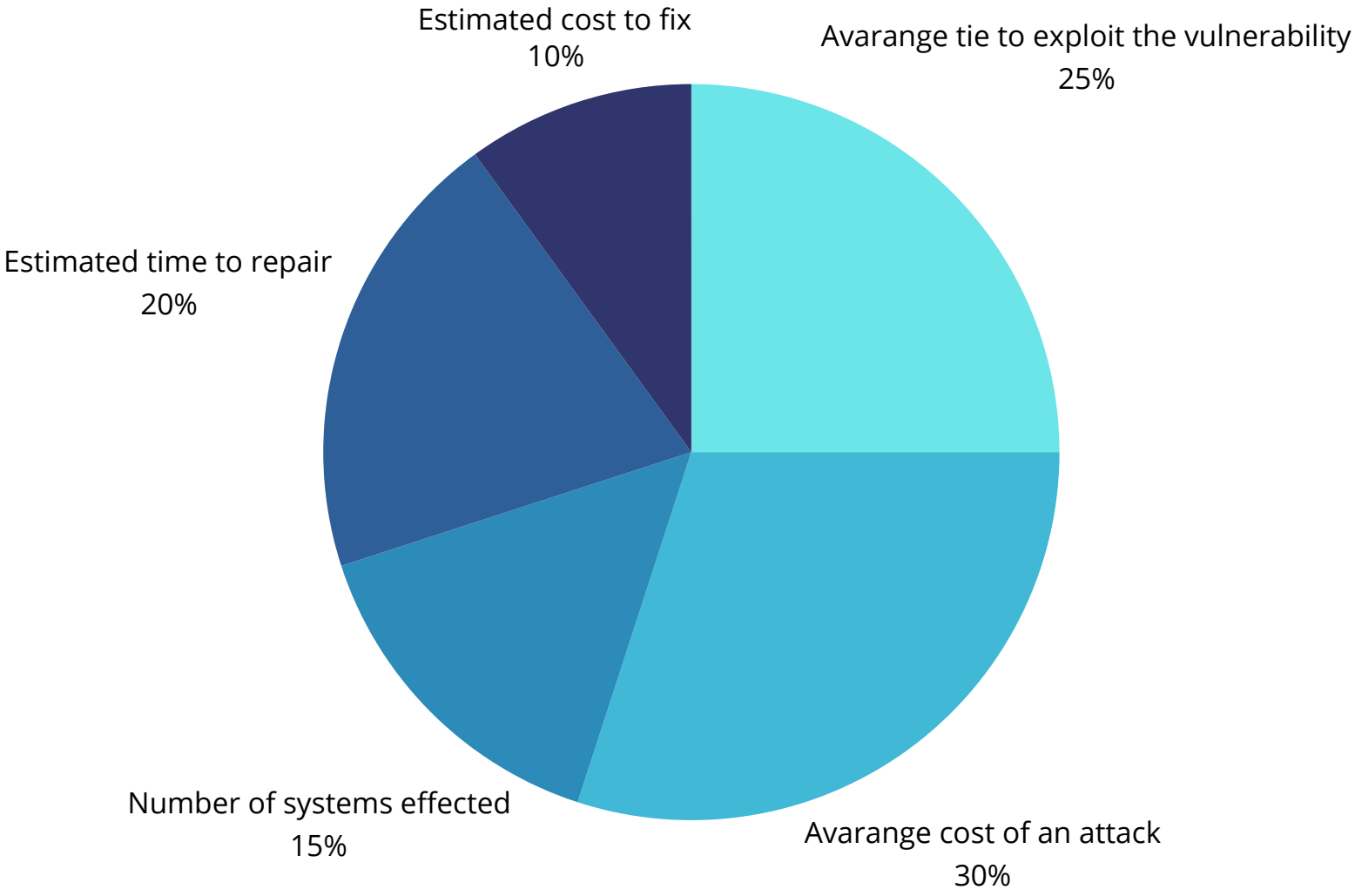
The potential economic savings for the single vulnerability can be calculated ad follows:

Economic savings = (30 days / 7 days) * (50.000euro * 10) + 5.000 euro
Economic savings = (4,29) * (5000.000) + 5.000 euro
Economic savings ≈ 2.145.000 + 5.000 euro
Economic savings ≈ 2.150.000

To calculate the total economic losses associated with all the indicated vulnerabilities, we would sum up the economic savings calculated for each vulnerability.

Tolal economic savings ≈ 14 * 2.150.000 euro

Tolal economic savings ≈ 30.100.000 euro


Estimated cost to fix
10%
Avarange tie to exploit the vulnerability
25%
Estimated time to repair
20%
Number of systems effected
15%
Avarange cost of an attack
30%

192.168.1.131

9	3	9	6	89
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Thu May 9 15:22:39
End time:	2024 Thu May 9 15:48:01 2024

Host Information

IP:	192.168.1.131
MAC Address:	08:00:27:52:AD:CA
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Synopsis There is a vulnerable AJP connector listening on the remote host.

Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

Solution Update the AJP configuration to require authorization and/or upgrade the Tomcat server to

7.0.100, 8.5.51,
9.0.31 or later.

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

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.5 (CVSS2#E:H/RL:OF/RC:C)

Reference

s CVE	CVE-2020-1745 CVE-2020-1938 CISA-
CVE	KNOWN-EXPLOITED:2022/03/17
XREF	CEA-ID:CEA-2020-0021
XREF	

Plugin Information

Published: 2020/03/24, Modified: 2024/03/19

Plugin Output

tcp/8009/ajp13

```
Nessus was able to exploit the issue using the following request :           ....HTTP/1.1.../
                                                                             asdf/xxxxx.jsp..
0x0000: 02 02 00 08 48 54 54 50 2F 31 2E 31 00 00 0F 2F 0x0010: 61
73 64 66 2F 78 78 78 78 78 2E 6A 73 70 00 00
```

```
0x0020: 09 6C 6F 63 61 6C 68 6F 73 74 00 FF FF 00 09 6C           .localhost.....l
0x0030: 6F 63 61 6C 68 6F 73 74 00 00 50 00 00 09 A0 06           ocalhost..P.....
0x0040: 00 0A 6B 65 65 70 2D 61 6C 69 76 65 00 00 0F 41           ..keep-alive...A
0x0050: 63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 00 00           ccept-Language..
0x0060: 0E 65 6E 2D 55 53 2C 65 6E 3B 71 3D 30 2E 35 00           .en-US,en;q=0.5.
0x0070: A0 08 00 01 30 00 00 0F 41 63 63 65 70 74 2D 45           ....0...Accept-E
0x0080: 6E 63 6F 64 69 6E 67 00 00 13 67 7A 69 70 2C 20           ncoding...gzip,
0x0090: 64 65 66 6C 61 74 65 2C 20 73 64 63 68 00 00 0D           deflate, sdch...
0x00A0: 43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C 00 00 09           Cache-Control...
0x00B0: 6D 61 78 2D 61 67 65 3D 30 00 A0 0E 00 07 4D 6F           max-age=0.....Mo
0x00C0: 7A 69 6C 6C 61 00 00 19 55 70 67 72 61 64 65 2D           zilla...Upgrade-
0x00D0: 49 6E 73 65 63 75 72 65 2D 52 65 71 75 65 73 74           Insecure-Request
0x00E0: 73 00 00 01 31 00 A0 01 00 09 74 65 78 74 2F 68           s...1.....text/h
0x00F0: 74 6D 6C 00 A0 0B 00 09 6C 6F 63 61 6C 68 6F 73           tml.....localhos
0x0100: 74 00 0A 00 21 6A 61 76 61 78 2E 73 65 72 76 6C           t...!javax.servl
0x0110: 65 74 2E 69 6E 63 6C 75 64 65 2E 72 65 71 75 65           et.include.reque
0x0120: 73 74 5F 75 72 69 00 00 01 31 00 0A 00 1F 6A 61           st_uri...1....ja
0x0130: 76 61 78 2E 73 65 72 76 6C 65 74 2E 69 6E 63 6C           vax.servlet.incl
0x0140: 75 64 65 2E 70 61 74 68 5F 69 6E 66 6F 00 00 10           ude.path_info...
0x0150: 2F 57 45 42 2D 49 4E 46 2F 77 65 62 2E 78 6D 6C           /WEB-INF/web.xml
0x0160: 00 0A 00 22 6A 61 76 61 78 2E 73 65 72 76 6C 65           ..."javax.servle
0x0170: 74 2E 69 6E 63 6C 75 64 65 2E 73 65 72 76 6C 65           t.include.servle
0x0180: 74 5F 70 61 74 68 00 00 00 00 FF                          t_path.....



This produced the following truncated output (limite [...]
```

171340 - Apache Tomcat SEoL (<= 5.5.x)

Synopsis An unsupported version of Apache Tomcat is installed on the remote host.

Description

According to its version, Apache Tomcat is less than or equal to 5.5.x. It is, therefore, no longer maintained by its vendor or provider.
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Upgrade to a version of Apache Tomcat that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2023/02/10, Modified: 2024/05/06

Plugin Output

tcp/8180/www

```
 URL                                   : http://192.168.1.131:8180/
Installed version                      : 5.5
Security End of Life                   : September 30, 2012
Time since Security End of Life (Est.) : >= 11 years
```

51988 - Bind Shell Backdoor Detection

Synopsis The remote host may have been compromised.

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.

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 v2.0 Base Score

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

Plugin Information

Published: 2011/02/15, Modified: 2022/04/11

Plugin Output

tcp/1524/wild_shell

```
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 ------------------------------
```

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Synopsis

The remote SSH host keys are weak.

Description

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.
The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.
An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor

Critical

VPR Score

5.1

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	29179
CVE	CVE-2008-0166
XREF	CWE:310

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/05/14, Modified: 2018/11/15

Plugin Output

tcp/22/ssh

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Synopsis

The remote SSL certificate uses a weak key.

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.
The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.
An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor

Critical

VPR Score

5.1

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	29179
CVE	CVE-2008-0166
XREF	CWE:310

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/05/15, Modified: 2020/11/16

Plugin Output

tcp/5432/postgresql

20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

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.

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 v2.0 Base Score

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

Plugin Information

Published: 2005/10/12, Modified: 2022/04/04

Plugin Output

tcp/5432/postgresql

```
- SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX           Auth     Encryption
    ----------------------        ----------        ---           ----     MAC  ----------------------
    EDH-RSA-DES-CBC3-SHA                            DH            RSA      --- 3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                                    RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption
    ----------------------        ----------        ---           ----     MAC  ----------------------
    DHE-RSA-AES128-SHA                              DH            RSA      --- AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA                              DH            RSA      AES-CBC(256)
 SHA1
    AES128-SHA                                      RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                                      RSA           RSA      AES-CBC(256)
 SHA1
    RC4-SHA                                         RSA           RSA      RC4(128)
 SHA1

The fields above are :

  {Tenable ciphername}
 {Cipher ID code}
 Kex={key exchange}
 Auth={authentication}
 Encrypt={symmetric encryption method}
 MAC={message authentication code}
 {export flag}
```

33850 - Unix Operating System Unsupported Version Detection

Synopsis

The operating system running on the remote host is no longer supported.

Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a version of the Unix operating system that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Reference

s XREF	IAVA:0001-A-0502 IAVA:0001-A-0648
XREF	

Plugin Information

Published: 2008/08/08, Modified: 2024/04/03

Plugin Output

tcp/0

```
Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server).
Upgrade to Ubuntu 23.04 / LTS 22.04 / LTS 20.04 .

For more information, see : https://wiki.ubuntu.com/Releases
```

46882 - UnrealIRCd Backdoor Detection

Synopsis

The remote IRC server contains a backdoor.

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.

Risk Factor

Critical

VPR Score

7.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	40820
CVE	CVE-2010-2075

Exploitable With

CANVAS (true) Metasploit (true)

Plugin Information

Published: 2010/06/14, Modified: 2022/04/11

Plugin Output

tcp/6667/irc

```
The remote IRC server is running as :

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

61708 - VNC Server 'password' Password

Synopsis

A VNC server running on the remote host is secured with a weak password.

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.

Risk Factor

Critical

CVSS v2.0 Base Score

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

Plugin Information

Published: 2012/08/29, Modified: 2015/09/24

Plugin Output

tcp/5900/vnc

```
Nessus logged in using a password of "password".
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

5.1

CVSS v2.0 Base Score

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

References

CVE	CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/5432/postgresql

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code ------      KEX           Auth     ~~MAC~~Cryption----------------
    ----------------------        ----  0x00,      ---           ----     --- 3DES-CBC(168)
    EDH-RSA-DES-CBC3-SHA          0x16             DH            RSA
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

The fields above are :

  {Tenable ciphername}
 {Cipher ID code}
 Kex={key exchange}
 Auth={authentication}
 Encrypt={symmetric encryption method}
 MAC={message authentication code}
 {export flag}
```

10205 - rlogin Service Detection

Synopsis

The rlogin service is running on the remote host.

Description

The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication.

Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Solution

Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

Risk Factor

High

VPR Score

5.9

CVSS v2.0 Base Score

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

References

CVE CVE-1999-0651

Exploitable With

Metasploit

(true)

Plugin Information

Published: 1999/08/30, Modified: 2022/04/11

Plugin Output

tcp/513/rlogin

10245 - rsh Service Detection

Synopsis

The rsh service is running on the remote host.

Description

The rsh service is running on the remote host. This service is vulnerable since data is passed between the rsh client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication.

Finally, rsh is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Solution

Comment out the 'rsh' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

Risk Factor

High

VPR Score

5.9

CVSS v2.0 Base Score

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

References

CVE CVE-1999-0651

Exploitable With

Metasploit

(true)

Plugin Information

Published: 1999/08/22, Modified: 2022/04/11

Plugin Output

tcp/514/rsh