Derpnstink

Report generated by Nessus™ Thu, 22 Jun 2023 13:17:36 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.1.112

8	1	1	3	38
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Thu Jun 22 13:15:21 2023
End time: Thu Jun 22 13:17:36 2023

Host Information

DNS Name: derpnstink.local
IP: 192.168.1.112
MAC Address: 08:00:27:61:CD:5B
OS: Linux Kernel 3.13 on Ubuntu 14.04 (trusty)

Vulnerabilities

156164 - Apache Log4Shell CVE-2021-45046 Bypass Remote Code Execution

Synopsis

The version of Apache Log4j used on the remote server is affected by a remote code execution vulnerability.

Description

A remote code execution vulnerability exists in Apache Log4j < 2.16.0 due to insufficient protections on message lookup substitutions when dealing with user controlled input. A remote, unauthenticated attacker can explolit this, via a web request to execute arbitrary code with the permission level of the running Java process.

Note that this bypass requires a non-default configuration. Only Pattern Layouts with a Context Lookup (for example, $${ctx:loginId}) are vulnerable to this.

This plugin requires that both the scanner and target machine have internet access.

See Also

https://logging.apache.org/log4j/2.x/security.html

https://www.lunasec.io/docs/blog/log4j-zero-day/

http://www.nessus.org/u?a0e621e5

Solution

Upgrade to Apache Log4j version 2.16.0 or later, or apply the vendor mitigation.

Upgrading to the latest versions for Apache Log4j is highly recommended as intermediate versions / patches have known high severity vulnerabilities and the vendor is updating their advisories often as new research and knowledge about the impact of Log4j is discovered. Refer to https://logging.apache.org/log4j/2.x/security.html for the latest versions.

Risk Factor

High

CVSS v3.0 Base Score

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

VPR Score

9.2

CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

STIG Severity

I

References

CVE	CVE-2021-45046
XREF	IAVA:2021-A-0573
XREF	IAVA:2021-A-0598
XREF	IAVA:0001-A-0650

Plugin Information

Published: 2021/12/17, Modified: 2023/05/31

Plugin Output

tcp/80/www

```
Nessus was able to detect the vulnerability by sending the following request

GET / HTTP/1.1
Host: derpnstink.local
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: ${jndi:ldap://127.0.0.1#log4shell-generic-5ZJIt0bCPVTWuYncDKyI.w.nessus.org/nessus}
```

```
Connection: Keep-Alive
Referer: ${jndi:ldap://127.0.0.1#log4shell-generic-5ZJIt0bCPVTWuYncDKyI.w.nessus.org/nessus}
X-Api-Version: ${jndi:ldap://127.0.0.1#log4shell-generic-5ZJIt0bCPVTWuYncDKyI.w.nessus.org/nessus}
Cookie: ${jndi:ldap://127.0.0.1#log4shell-generic-5ZJIt0bCPVTWuYncDKyI.w.nessus.org/nessus}=
${jndi:ldap://127.0.0.1#log4shell-generic-5ZJIt0bCPVTWuYncDKyI.w.nessus.org/nessus};JSESSIONID=
${jndi:ldap://127.0.0.1#log4shell-generic-5ZJIt0bCPVTWuYncDKyI.w.nessus.org/nessus};SESSIONID=
${jndi:ldap://127.0.0.1#log4shell-generic-5ZJIt0bCPVTWuYncDKyI.w.nessus.org/nessus};PHPSESSID=
${jndi:ldap://127.0.0.1#log4shell-generic-5ZJIt0bCPVTWuYncDKyI.w.nessus.org/nessus};token=
${jndi:ldap://127.0.0.1#log4shell-generic-5ZJIt0bCPVTWuYncDKyI.w.nessus.org/nessus};session=
${jndi:ldap://127.0.0.1#log4shell-generic-5ZJIt0bCPVTWuYncDKyI.w.nessus.org/nessus}
User-Agent: ${jndi:ldap://127.0.0.1#log4shell-generic-5ZJIt0bCPVTWuYncDKyI.w.nessus.org/nessus}
Pragma: no-cache
If-Modified-Since: ${jndi:ldap://127.0.0.1#log4shell-generic-5ZJIt0bCPVTWuYncDKyI.w.nessus.org/
nessus}
Accept: ${jndi:ldap://127.0.0.1#log4shell-generic-5ZJIt0bCPVTWuYncDKyI.w.nessus.org/nessus}
Nessus detected that the target host performed a DNS lookup on an LDAP host.
```

156016 - Apache Log4Shell RCE detection via Path Enumeration (Direct Check HTTP)

Synopsis

The remote web server is affected by a remote code execution vulnerability.

Description

The remote web server is affected by a remote code execution vulnerability via a flaw in the Apache Log4j library. The vulnerability is due to the processing of unsanitized input sent to a logging function. A remote, unauthenticated attacker can explolit this, via a web request to execute arbitrary code with the permission level of the running Java process.

See Also

https://logging.apache.org/log4j/2.x/security.html

https://www.lunasec.io/docs/blog/log4j-zero-day/

Solution

Upgrade to Apache Log4j version 2.15.0 or later, or apply the vendor mitigation.

Upgrading to the latest versions for Apache Log4j is highly recommended as intermediate versions / patches have known high severity vulnerabilities and the vendor is updating their advisories often as new research and knowledge about the impact of Log4j is discovered. Refer to https://logging.apache.org/log4j/2.x/security.html for the latest versions.

Risk Factor

High

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 v3.0 Temporal Score

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

VPR Score

10.0

CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-44228
XREF	IAVA:2021-A-0573
XREF	IAVA:2021-A-0596
XREF	IAVA:2021-A-0597
XREF	IAVA:2021-A-0598
XREF	IAVA:0001-A-0650
XREF	CISA-KNOWN-EXPLOITED:2021/12/24
XREF	CEA-ID:CEA-2021-0052
XREF	CEA-ID:CEA-2023-0004

Exploitable With

CANVAS (true) Core Impact (true)

Plugin Information

Published: 2021/12/12, Modified: 2023/05/31

Plugin Output

tcp/80/www

```
Nessus was able to detect vulnerability by sending the following request

GET / HTTP/1.1
Host: derpnstink.local
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: ${jndi:ldap://log4shell-generic-sHjjzSnUHtc3d4n2aNwK${lower:ten}.w.nessus.org/
nessus}
Connection: Keep-Alive
Referer: ${jndi:ldap://log4shell-generic-sHjjzSnUHtc3d4n2aNwK${lower:ten}.w.nessus.org/nessus}
X-Api-Version: ${jndi:ldap://log4shell-generic-sHjjzSnUHtc3d4n2aNwK${lower:ten}.w.nessus.org/nessus}
Cookie: ${jndi:ldap://log4shell-generic-sHjjzSnUHtc3d4n2aNwK${lower:ten}.w.nessus.org/nessus}=
${jndi:ldap://log4shell-generic-sHjjzSnUHtc3d4n2aNwK${lower:ten}.w.nessus.org/nessus};JSESSIONID=
${jndi:ldap://log4shell-generic-sHjjzSnUHtc3d4n2aNwK${lower:ten}.w.nessus.org/nessus};SESSIONID=
${jndi:ldap://log4shell-generic-sHjjzSnUHtc3d4n2aNwK${lower:ten}.w.nessus.org/nessus};PHPSESSID=
${jndi:ldap://log4shell-generic-sHjjzSnUHtc3d4n2aNwK${lower:ten}.w.nessus.org/nessus};token=
${jndi:ldap://log4shell-generic-sHjjzSnUHtc3d4n2aNwK${lower:ten}.w.nessus.org/nessus};session=
${jndi:ldap://log4shell-generic-sHjjzSnUHtc3d4n2aNwK${lower:ten}.w.nessus.org/nessus}
User-Agent: ${jndi:ldap://log4shell-generic-sHjjzSnUHtc3d4n2aNwK${lower:ten}.w.nessus.org/nessus}
Pragma: no-cache
If-Modified-Since: ${jndi:ldap://log4shell-generic-sHjjzSnUHtc3d4n2aNwK${lower:ten}.w.nessus.org/
nessus}
Accept: ${jndi:ldap://log4shell-generic-sHjjzSnUHtc3d4n2aNwK${lower:ten}.w.nessus.org/nessus}
Nessus detected that the target host performed a DNS lookup on a LDAP host.
```

156056 - Apache Log4Shell RCE detection via Raw Socket Logging (Direct Check)

Synopsis

The version of Apache Log4j used on the remote server is affected by a remote code execution vulnerability.

Description

A remote code execution vulnerability exists in Apache Log4j < 2.15.0 due to insufficient protections on message lookup substitutions when dealing with user controlled input. A remote, unauthenticated attacker can explolit this, via a web request to execute arbitrary code with the permission level of the running Java process.

This plugin sends a test string to a set of open ports on the target host. This plugin requires that both the scanner and target machine have internet access.

See Also

https://logging.apache.org/log4j/2.x/security.html

https://www.lunasec.io/docs/blog/log4j-zero-day/

Solution

Upgrade to Apache Log4j version 2.15.0 or later, or apply the vendor mitigation.

Upgrading to the latest versions for Apache Log4j is highly recommended as intermediate versions / patches have known high severity vulnerabilities and the vendor is updating their advisories often as new research and knowledge about the impact of Log4j is discovered. Refer to https://logging.apache.org/log4j/2.x/security.html for the latest versions.

Risk Factor

High

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 v3.0 Temporal Score

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

VPR Score

10.0

CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-44228
XREF	IAVA:2021-A-0573
XREF	IAVA:2021-A-0596
XREF	IAVA:2021-A-0597
XREF	IAVA:2021-A-0598
XREF	IAVA:0001-A-0650
XREF	CISA-KNOWN-EXPLOITED:2021/12/24
XREF	CEA-ID:CEA-2021-0052
XREF	CEA-ID:CEA-2023-0004

Exploitable With

CANVAS (true) Core Impact (true)

Plugin Information

Published: 2021/12/14, Modified: 2023/05/31

Plugin Output

tcp/21/ftp

```
Nessus was able to detect the vulnerability by sending the following request

${jndi:ldap://log4shell-generic-gN7XxDVNJ1t1sFJmYagb${lower:ten}.w.nessus.org/nessus}Nessus detected
 that the target host performed a DNS lookup on an LDAP host.
```

156056 - Apache Log4Shell RCE detection via Raw Socket Logging (Direct Check)

Synopsis

The version of Apache Log4j used on the remote server is affected by a remote code execution vulnerability.

Description

A remote code execution vulnerability exists in Apache Log4j < 2.15.0 due to insufficient protections on message lookup substitutions when dealing with user controlled input. A remote, unauthenticated attacker can explolit this, via a web request to execute arbitrary code with the permission level of the running Java process.

This plugin sends a test string to a set of open ports on the target host. This plugin requires that both the scanner and target machine have internet access.

See Also

https://logging.apache.org/log4j/2.x/security.html

https://www.lunasec.io/docs/blog/log4j-zero-day/

Solution

Upgrade to Apache Log4j version 2.15.0 or later, or apply the vendor mitigation.

Upgrading to the latest versions for Apache Log4j is highly recommended as intermediate versions / patches have known high severity vulnerabilities and the vendor is updating their advisories often as new research and knowledge about the impact of Log4j is discovered. Refer to https://logging.apache.org/log4j/2.x/security.html for the latest versions.

Risk Factor

High

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 v3.0 Temporal Score

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

VPR Score

10.0

CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-44228
XREF	IAVA:2021-A-0573
XREF	IAVA:2021-A-0596
XREF	IAVA:2021-A-0597
XREF	IAVA:2021-A-0598
XREF	IAVA:0001-A-0650
XREF	CISA-KNOWN-EXPLOITED:2021/12/24
XREF	CEA-ID:CEA-2021-0052
XREF	CEA-ID:CEA-2023-0004

Exploitable With

CANVAS (true) Core Impact (true)

Plugin Information

Published: 2021/12/14, Modified: 2023/05/31

Plugin Output

tcp/22/ssh

```
Nessus was able to detect the vulnerability by sending the following request

${jndi:ldap://log4shell-generic-rbcyCfzb33f4UGvHPB05${lower:ten}.w.nessus.org/nessus}Nessus detected
 that the target host performed a DNS lookup on an LDAP host.
```

156056 - Apache Log4Shell RCE detection via Raw Socket Logging (Direct Check)

Synopsis

The version of Apache Log4j used on the remote server is affected by a remote code execution vulnerability.

Description

A remote code execution vulnerability exists in Apache Log4j < 2.15.0 due to insufficient protections on message lookup substitutions when dealing with user controlled input. A remote, unauthenticated attacker can explolit this, via a web request to execute arbitrary code with the permission level of the running Java process.

This plugin sends a test string to a set of open ports on the target host. This plugin requires that both the scanner and target machine have internet access.

See Also

https://logging.apache.org/log4j/2.x/security.html

https://www.lunasec.io/docs/blog/log4j-zero-day/

Solution

Upgrade to Apache Log4j version 2.15.0 or later, or apply the vendor mitigation.

Upgrading to the latest versions for Apache Log4j is highly recommended as intermediate versions / patches have known high severity vulnerabilities and the vendor is updating their advisories often as new research and knowledge about the impact of Log4j is discovered. Refer to https://logging.apache.org/log4j/2.x/security.html for the latest versions.

Risk Factor

High

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 v3.0 Temporal Score

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

VPR Score

10.0

CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-44228
XREF	IAVA:2021-A-0573
XREF	IAVA:2021-A-0596
XREF	IAVA:2021-A-0597
XREF	IAVA:2021-A-0598
XREF	IAVA:0001-A-0650
XREF	CISA-KNOWN-EXPLOITED:2021/12/24
XREF	CEA-ID:CEA-2021-0052
XREF	CEA-ID:CEA-2023-0004

Exploitable With

CANVAS (true) Core Impact (true)

Plugin Information

Published: 2021/12/14, Modified: 2023/05/31

Plugin Output

tcp/80/www

```
Nessus was able to detect the vulnerability by sending the following request

${jndi:ldap://log4shell-generic-vNlRVXKOoDFEacqTKBvp${lower:ten}.w.nessus.org/nessus}Nessus detected
 that the target host performed a DNS lookup on an LDAP host.
```

156115 - Apache Log4Shell RCE detection via callback correlation (Direct Check FTP)

Synopsis

The version of Apache Log4j used on the remote server is affected by a remote code execution vulnerability.

Description

A remote code execution vulnerability exists in Apache Log4j < 2.15.0 due to insufficient protections on message lookup substitutions when dealing with user controlled input. A remote, unauthenticated attacker can explolit this, via a web request to execute arbitrary code with the permission level of the running Java process.

See Also

https://logging.apache.org/log4j/2.x/security.html

https://www.lunasec.io/docs/blog/log4j-zero-day/

Solution

Upgrade to Apache Log4j version 2.15.0 or later, or apply the vendor mitigation.

Upgrading to the latest versions for Apache Log4j is highly recommended as intermediate versions / patches have known high severity vulnerabilities and the vendor is updating their advisories often as new research and knowledge about the impact of Log4j is discovered. Refer to https://logging.apache.org/log4j/2.x/security.html for the latest versions.

Risk Factor

High

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 v3.0 Temporal Score

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

VPR Score

10.0

CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-44228
XREF	IAVA:2021-A-0573
XREF	IAVA:2021-A-0598
XREF	IAVA:0001-A-0650
XREF	CISA-KNOWN-EXPLOITED:2021/12/24
XREF	CEA-ID:CEA-2021-0052
XREF	CEA-ID:CEA-2023-0004

Exploitable With

CANVAS (true) Core Impact (true)

Plugin Information

Published: 2021/12/16, Modified: 2023/06/12

Plugin Output

tcp/21/ftp

```
Nessus was able to detect the vulnerability by sending FTP commands with a benign payload in it.
Nessus detected that the target host performed a DNS lookup on a name in the payload.
```

156014 - Apache Log4Shell RCE detection via callback correlation (Direct Check HTTP)

Synopsis

The version of Apache Log4j used on the remote server is affected by a remote code execution vulnerability.

Description

A remote code execution vulnerability exists in Apache Log4j < 2.15.0 due to insufficient protections on message lookup substitutions when dealing with user controlled input. A remote, unauthenticated attacker can explolit this, via a web request to execute arbitrary code with the permission level of the running Java process.

This plugin requires that both the scanner and target machine have internet access.

See Also

https://logging.apache.org/log4j/2.x/security.html

https://www.lunasec.io/docs/blog/log4j-zero-day/

Solution

Upgrade to Apache Log4j version 2.15.0 or later, or apply the vendor mitigation.

Upgrading to the latest versions for Apache Log4j is highly recommended as intermediate versions / patches have known high severity vulnerabilities and the vendor is updating their advisories often as new research and knowledge about the impact of Log4j is discovered. Refer to https://logging.apache.org/log4j/2.x/security.html for the latest versions.

Risk Factor

High

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 v3.0 Temporal Score

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

VPR Score

10.0

CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-44228
XREF	IAVA:2021-A-0573
XREF	IAVA:2021-A-0596
XREF	IAVA:2021-A-0597
XREF	IAVA:2021-A-0598
XREF	IAVA:0001-A-0650
XREF	CISA-KNOWN-EXPLOITED:2021/12/24
XREF	CEA-ID:CEA-2021-0052
XREF	CEA-ID:CEA-2023-0004

Exploitable With

CANVAS (true) Core Impact (true)

Plugin Information

Published: 2021/12/11, Modified: 2023/05/31

Plugin Output

tcp/80/www

```
Nessus was able to detect vulnerability by sending the following request

GET / HTTP/1.1
Host: derpnstink.local
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: ${jndi:ldap://log4shell-generic-xO84VuVvgEZ4fEaJ2cxV${lower:ten}.w.nessus.org/
nessus}
Connection: Keep-Alive
Referer: ${jndi:ldap://log4shell-generic-xO84VuVvgEZ4fEaJ2cxV${lower:ten}.w.nessus.org/nessus}
X-Api-Version: ${jndi:ldap://log4shell-generic-xO84VuVvgEZ4fEaJ2cxV${lower:ten}.w.nessus.org/nessus}
Cookie: ${jndi:ldap://log4shell-generic-xO84VuVvgEZ4fEaJ2cxV${lower:ten}.w.nessus.org/nessus}=
${jndi:ldap://log4shell-generic-xO84VuVvgEZ4fEaJ2cxV${lower:ten}.w.nessus.org/nessus};JSESSIONID=
${jndi:ldap://log4shell-generic-xO84VuVvgEZ4fEaJ2cxV${lower:ten}.w.nessus.org/nessus};SESSIONID=
${jndi:ldap://log4shell-generic-xO84VuVvgEZ4fEaJ2cxV${lower:ten}.w.nessus.org/nessus};PHPSESSID=
${jndi:ldap://log4shell-generic-xO84VuVvgEZ4fEaJ2cxV${lower:ten}.w.nessus.org/nessus};token=
${jndi:ldap://log4shell-generic-xO84VuVvgEZ4fEaJ2cxV${lower:ten}.w.nessus.org/nessus};session=
${jndi:ldap://log4shell-generic-xO84VuVvgEZ4fEaJ2cxV${lower:ten}.w.nessus.org/nessus}
User-Agent: ${jndi:ldap://log4shell-generic-xO84VuVvgEZ4fEaJ2cxV${lower:ten}.w.nessus.org/nessus}
Pragma: no-cache
If-Modified-Since: ${jndi:ldap://log4shell-generic-xO84VuVvgEZ4fEaJ2cxV${lower:ten}.w.nessus.org/
nessus}
```

```
Accept: ${jndi:ldap://log4shell-generic-xO84VuVvgEZ4fEaJ2cxV${lower:ten}.w.nessus.org/nessus}
Nessus detected that the target host performed a DNS lookup on an LDAP host.
```

156166 - Apache Log4Shell RCE detection via callback correlation (Direct Check SSH)

Synopsis

The remote SSH service allows remote command execution via Log4Shell.

Description

The remote host appears to be running SSH. SSH itself is not vulnerable to Log4Shell; however, the SSH server could potentially be affected if it attempts to log data via a vulnerable log4j library.

This plugin requires that both the scanner and target machine have internet access.

See Also

https://logging.apache.org/log4j/2.x/security.html

https://www.lunasec.io/docs/blog/log4j-zero-day/

Solution

Upgrade to Apache Log4j version 2.15.0 or later, or apply the vendor mitigation.

Upgrading to the latest versions for Apache Log4j is highly recommended as intermediate versions / patches have known high severity vulnerabilities and the vendor is updating their advisories often as new research and knowledge about the impact of Log4j is discovered. Refer to https://logging.apache.org/log4j/2.x/security.html for the latest versions.

Risk Factor

High

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 v3.0 Temporal Score

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

VPR Score

10.0

CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-44228
XREF	IAVA:2021-A-0573
XREF	IAVA:0001-A-0650
XREF	CISA-KNOWN-EXPLOITED:2021/12/24
XREF	CEA-ID:CEA-2021-0052
XREF	CEA-ID:CEA-2023-0004

Exploitable With

CANVAS (true) Core Impact (true)

Plugin Information

Published: 2021/12/17, Modified: 2023/06/12

Plugin Output

tcp/22/ssh

```
Nessus was able to detect the vulnerability by trying to inject in various SSH protocol fields,
 as well as attempting to log in as user:${jndi:ldap://log4shell-ssh-4XkAa5PZ6XmKfymCbIxv
${lower:ten}.w.nessus.org/nessus}, password:${jndi:ldap://log4shell-ssh-4XkAa5PZ6XmKfymCbIxv
${lower:ten}.w.nessus.org/nessus}

Nessus detected that the target host then performed a DNS lookup on an LDAP host.
```

164017 - NodeJS System Information Library Command Injection (CVE-2021-21315)

Synopsis

The remote host contains a web application framework library that is affected by a command injection vulnerability.

Description

The remote host contains a systeminformation npm module that is prior to 5.3.1. It is, therefore, affected by a command injection vulnerability. The System Information Library for Node.JS (npm package 'systeminformation') is an open source collection of functions to retrieve detailed hardware, system and OS information. In systeminformation before version 5.3.1 there is a command injection vulnerability. The vulnerability was fixed in version 5.3.1. As a workaround instead of upgrading, be sure to check or sanitize service parameters that are passed to si.inetLatency(), si.inetChecksite(), si.services(), or si.processLoad()... to only allow strings and reject any arrays. String sanitization works as expected.

See Also

http://www.nessus.org/u?103e42ce

https://security.netapp.com/advisory/ntap-20210312-0007/

http://www.nessus.org/u?5b30aacc

http://www.nessus.org/u?103e42ce

Solution

Upgrade to the systeminformation module to 5.3.1 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

VPR Score

7.4

CVSS v2.0 Base Score

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

References

CVE	CVE-2021-21315

Plugin Information

Published: 2022/08/10, Modified: 2023/05/31

Plugin Output

tcp/80/www

```
Nessus was able to detect the vulnerability by a specially crafted payload.
Nessus detected that the target host performed a DNS lookup on a name in the payload.
```

90317 - SSH Weak Algorithms Supported

Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

See Also

https://tools.ietf.org/html/rfc4253#section-6.3

Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

Risk Factor

Medium

CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2016/04/04, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

```
The following weak server-to-client encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256

The following weak client-to-server encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256
```

70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor

Low

VPR Score

2.5

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS v2.0 Temporal Score

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

References

BID	32319
CVE	CVE-2008-5161
XREF	CERT:958563
XREF	CWE:200

Plugin Information

Published: 2013/10/28, Modified: 2018/07/30

Plugin Output

tcp/22/ssh

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
```

153953 - SSH Weak Key Exchange Algorithms Enabled

Synopsis

The remote SSH server is configured to allow weak key exchange algorithms.

Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

See Also

http://www.nessus.org/u?b02d91cd

https://datatracker.ietf.org/doc/html/rfc8732

Solution

Contact the vendor or consult product documentation to disable the weak algorithms.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2021/10/13, Modified: 2021/10/13

Plugin Output

tcp/22/ssh

```
The following weak key exchange algorithms are enabled :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group1-sha1
```

71049 - SSH Weak MAC Algorithms Enabled

Synopsis

The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

Risk Factor

Low

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin Information

Published: 2013/11/22, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

```
The following client-to-server Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com

The following server-to-client Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com
```

18261 - Apache Banner Linux Distribution Disclosure

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.

Risk Factor

None

Plugin Information

Published: 2005/05/15, Modified: 2022/03/21

Plugin Output

tcp/0

```
The Linux distribution detected was :
 - Ubuntu 14.04 (trusty)
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/05/24

Plugin Output

tcp/80/www

```
URL        : http://192.168.1.112/
Version    : 2.4.99
Source     : Server: Apache/2.4.7 (Ubuntu)
backported : 1
os         : ConvertedUbuntu
```

166602 - Asset Attribute: Fully Qualified Domain Name (FQDN)

Synopsis

Report Fully Qualified Domain Name (FQDN) for the remote host.

Description

Report Fully Qualified Domain Name (FQDN) for the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/10/27, Modified: 2022/10/27

Plugin Output

tcp/0

```
The FQDN for the remote host has been determined to be:

  FQDN       : derpnstink.local
  Confidence : 60
  Resolves   : False
  Method     : rDNS Lookup: IP Address
```

39519 - Backported Security Patch Detection (FTP)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote FTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/21/ftp

```
Give Nessus credentials to perform local checks.
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22/ssh

```
Give Nessus credentials to perform local checks.
```

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/80/www

```
Give Nessus credentials to perform local checks.
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2023/06/08

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :

  cpe:/o:canonical:ubuntu_linux:14.04 -> Canonical Ubuntu Linux

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server:2.4.7 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:apache:http_server:2.4.99 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:openbsd:openssh:6.6 -> OpenBSD OpenSSH
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 95
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following card manufacturers were identified :

08:00:27:61:CD:5B : PCS Systemtechnik GmbH
```

86420 - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 08:00:27:61:CD:5B
```

10092 - FTP Server Detection

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2019/11/22

Plugin Output

tcp/21/ftp

```
The remote FTP banner is :

220 (vsFTPd 3.0.2)
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Based on the response to an OPTIONS request :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :

Apache/2.4.7 (Ubuntu)
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

```
192.168.1.112 resolves as derpnstink.local.
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Thu, 22 Jun 2023 17:17:01 GMT
  Server: Apache/2.4.7 (Ubuntu)
  Last-Modified: Sun, 12 Nov 2017 16:12:12 GMT
  ETag: "512-55dcb6aaa2f50"
  Accept-Ranges: bytes
  Content-Length: 1298
  Vary: Accept-Encoding
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<html >

<head>

    <meta charset="UTF-8">
```

```
    <title>DeRPnStiNK</title>

    <link rel="stylesheet" href="css/style.css">
<script type="text/javascript" src="http://ajax.googleapis.com/ajax/libs/jquery/1.7.1/
jquery.min.js"></script>
<script type="text/javascript" src="/is/js/release/kveik.1.4.24.js?1"></script>
<script type="text/info" src="/webnotes/info.txt"></script>
</head>

<body>
  <!-- particles.js container -->
<div id="particles-js"></div>

<!-- stats - count particles -->
<div class="count-particles">

</div>
<div class="divhead"
<h1 style="color:Purple; font-size:250%;">DeRPnStiNK</h1>
</div>
<div class="divpic">
<table>
    <tr>
        <td style="padding:5px">
            <img src="derp.png">
          </td>
            <td style="padding:5px">
            <img src="stinky.png">
             </td>
        </tr>
    </table>

</div>

<script src='js/particles.min.js'></script>
<script src="js/index.js"></script>

</body>
```

```
<div>
<div>
<div>
<div>
<div>
<div>
<div>
<div class=tryharder>
<div>
<div>
<div>
<div>
<div>
<div>
<--flag1(52E37291AEDF6A46D7D0BB8A6312F4F9F1AA4975C248C3F0E008CBA09D6E9166) -->
</div>
</div>
</div>
</div>
</div>
</div>
</div>
</div>
</div>
</div>
</div>
</div>
</div>
</div>



</html>
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2023/04/27

Plugin Output

icmp/0

```
The difference between the local and remote clocks is -2 seconds.
```

46215 - Inconsistent Hostname and IP Address

Synopsis

The remote host's hostname is not consistent with DNS information.

Description

The name of this machine either does not resolve or resolves to a different IP address.

This may come from a badly configured reverse DNS or from a host file in use on the Nessus scanning host.

As a result, URLs in plugin output may not be directly usable in a web browser and some web tests may be incomplete.

Solution

Fix the reverse DNS or host file.

Risk Factor

None

Plugin Information

Published: 2010/05/03, Modified: 2016/08/05

Plugin Output

tcp/0

```
The host name 'derpnstink.local' does not resolve to an IP address
```

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: 2023/05/31

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: 2023/05/31

Plugin Output

tcp/22/ssh

```
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: 2023/05/31

Plugin Output

tcp/80/www

```
Port 80/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.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- 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: 2023/04/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.5.2
Nessus build : 20009
Plugin feed version : 202306140450
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : Derpnstink
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.1.2
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 172.153 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Scan Start Date : 2023/6/22 13:15 EDT
Scan duration : 122 sec
Scan for malware : no
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2022/03/09

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 3.13 on Ubuntu 14.04 (trusty)
Confidence level : 95
Method : HTTP


The remote host is running Linux Kernel 3.13 on Ubuntu 14.04 (trusty)
```

117886 - OS Security Patch Assessment Not Available

Synopsis

OS Security Patch Assessment is not available.

Description

OS Security Patch Assessment is not available on the remote host.

This does not necessarily indicate a problem with the scan.

Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0515

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/0

```
The following issues were reported :

  - Plugin      : no_local_checks_credentials.nasl
    Plugin ID   : 110723
    Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
    Message     :
Credentials were not provided for detected SSH service.
```

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.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2023/06/13

Plugin Output

tcp/0

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


[ Apache Log4Shell RCE detection via callback correlation (Direct Check FTP) (156115) ]

+ Action to take : Upgrade to Apache Log4j version 2.15.0 or later, or apply the vendor mitigation.

Upgrading to the latest versions for Apache Log4j is highly recommended as intermediate versions /
 patches have known high severity vulnerabilities and the vendor is updating their advisories
 often as new research and knowledge about the impact of Log4j is discovered. Refer to https://
logging.apache.org/log4j/2.x/security.html for the latest versions.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).


[ NodeJS System Information Library Command Injection (CVE-2021-21315) (164017) ]

+ Action to take : Upgrade to the systeminformation module to 5.3.1 or later.
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2017/08/28

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha1
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group1-sha1
  diffie-hellman-group14-sha1
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521

The server supports the following options for server_host_key_algorithms :

  ecdsa-sha2-nistp256
  ssh-dss
  ssh-ed25519
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes128-gcm@openssh.com
  aes192-cbc
  aes192-ctr
  aes256-cbc
```

```
  aes256-ctr
  aes256-gcm@openssh.com
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  chacha20-poly1305@openssh.com
  rijndael-cbc@lysator.liu.se

The server supports the following options for encryption_algorithms_server_to_client :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes128-gcm@openssh.com
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  aes256-gcm@openssh.com
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  chacha20-poly1305@openssh.com
  rijndael-cbc@lysator.liu.se

The server supports the following options for mac_algorithms_client_to_server :

  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-ripemd160
  hmac-ripemd160-etm@openssh.com
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-ripemd160
  hmac-ripemd160-etm@openssh.com
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com
  hmac-sh [...]
```

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2021/01/19

Plugin Output

tcp/22/ssh

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0
```

153588 - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/22/ssh

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com
  hmac-sha1-etm@openssh.com

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com
  hmac-sha1-etm@openssh.com
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.8
SSH supported authentication : publickey
SSH banner :
Ubuntu 14.04.5 LTS


                      ,~~~~~~~~~~~~~..
                      '  Derrrrrp  N  `
        ,~~~~~~,      |    Stink      |
       / ,      \     ',  _________ _,"
      /,~|_______\.     \/
     /~ (__________)
    (*)  ; (^)(^)':
        =;  ____  ;
          ; """"  ;=
   {"}_   ' '""' ' _{"}
   \__/     >  <   \__/
      \    ,"   ",  /
       \  "       /"
          "      "=
           >     <
          ="     "-
          -`.   ,'
```

```
                -
            `--'
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/03/29

Plugin Output

tcp/21/ftp

```
An FTP server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/03/29

Plugin Output

tcp/22/ssh

```
An SSH server is running on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/03/29

Plugin Output

tcp/80/www

```
A web server is running on this port.
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/03/06

Plugin Output

tcp/0

110723 - Target Credential Status by Authentication Protocol - No Credentials Provided

Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2023/02/13

Plugin Output

tcp/0

```
SSH was detected on port 22 but no credentials were provided.
SSH local checks were not enabled.
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/05/03

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.2 to 192.168.1.112 :
192.168.1.2
192.168.1.112

Hop Count: 1
```

66293 - Unix Operating System on Extended Support

Synopsis

The remote host is running an operating system that is on extended support.

Description

According to its version, the remote host uses a Unix or Unix-like operating system that has transitioned to an extended portion in its support life cycle. Continued access to new security updates requires payment of an additional fee and / or configuration changes to the package management tool. Without that, the host likely will be missing security updates.

Solution

Ensure that the host subscribes to the vendor's extended support plan and continues to receive security updates.

Risk Factor

None

References

XREF	IAVA:0001-A-0648

Plugin Information

Published: 2013/05/02, Modified: 2023/05/10

Plugin Output

tcp/0

```
Ubuntu 14.04 support ends on 2019-04-30 (end of maintenance) / 2024-04-30 (end of extended security
 maintenance).
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/orig.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

tcp/80/www

```
Contents of robots.txt :

User-agent: *
Disallow: /php/
Disallow: /temporary/
```

66717 - mDNS Detection (Local Network)

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

This plugin attempts to discover mDNS used by hosts residing on the same network segment as Nessus.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

None

Plugin Information

Published: 2013/05/31, Modified: 2013/05/31

Plugin Output

udp/5353/mdns

```
Nessus was able to extract the following information :

  - mDNS hostname       : DeRPnStiNK.local.

  - Advertised services :
    o Service name      : DeRPnStiNK [08:00:27:61:cd:5b]._workstation._tcp.local.
      Port number       : 9

  - CPU type            : I686
  - OS                  : LINUX
```

52703 - vsftpd Detection

Synopsis

An FTP server is listening on the remote port.

Description

The remote host is running vsftpd, an FTP server for UNIX-like systems written in C.

See Also

http://vsftpd.beasts.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/03/17, Modified: 2019/11/22

Plugin Output

tcp/21/ftp

```
Source  : 220 (vsFTPd 3.0.2)
Version : 3.0.2
```