



وھبھ WEHBEH ساري. Sari
2023-12-14 11.11 AM

swe - 14-12-2023 - sweh - Sari ساري. WEHBEH وھبھ - file'test.pdf - 1.11.0 - Quality Assurance - 2

swe - 14-12-2023 - sweh - Sari ساري WEHBEH. و هبه - file'test.pdf - 1.11.0 - Quality Assurance - 2

swe - 14-12-2023 - sweh - Sari ساري WEHBEH. و هبه - file'test.pdf - 1.11.0 - Quality Assurance - 2

swe - 14-12-2023 - sweh - Sari ساري WEHBEH. و هبه - file'test.pdf - 1.11.0 - Quality Assurance - 2

swe - 14-12-2023 - sweh - Sari ساري WEHBEH. و هبه - file'test.pdf - 1.11.0 - Quality Assurance - 2

swe - 14-12-2023 - sweh - Sari ساري WEHBEH. و هبه - file'test.pdf - 1.11.0 - Quality Assurance - 2

swe - 14-12-2023 - sweh - Sari ساري WEHBEH. و هبه - file'test.pdf - 1.11.0 - Quality Assurance - 2

swe - 14-12-2023 - sweh - Sari ساري WEHBEH. وهبه - file'test.pdf - 1.11.0 - Quality Assurance - 2

swe - 14-12-2023 - sweh - Sari ساري WEHBEH. و هبه - file'test.pdf - 1.11.0 - Quality Assurance - 2

swe - 14-12-2023 - sweh - Sari ساري WEHBEH. و هبه - file'test.pdf - 1.11.0 - Quality Assurance - 2

swe - 14-12-2023 - sweh - Sari ساري WEHBEH. و هبه - file'test.pdf - 1.11.0 - Quality Assurance - 2

swe - 14-12-2023 - sweh - Sari ساري WEHBEH. و هبه - file'test.pdf - 1.11.0 - Quality Assurance - 2

swe - 14-12-2023 - sweh - Sari ساري WEHBEH. و هبه - file'test.pdf - 1.11.0 - Quality Assurance - 2

swe - 14-12-2023 - sweh - Sari ساري WEHBEH. و هبه - file'test.pdf - 1.11.0 - Quality Assurance - 2

swe - 14-12-2023 - sweh - Sari ساري WEHBEH. و هبه - file'test.pdf - 1.11.0 - Quality Assurance - 2

Log4Shell bug impacting Apache Log4j2 Report

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
156002	Apache Log4j < 2.15.0 Remote Code Execution (Windows)	Misc.	Critical	10.2.35.39	TCP	445
MAC Address: 00:50:56:80:25:12						
DNS Name: adkdcvdecmau1.ad.mohap.gov.ae						
NetBIOS Name: ad.mohap.gov.ae\ADKDCVDECEMAU1						
Plugin Output:						
Plugin Output:						
Path : D:\EBS\New_CTS\Intalio Document - 11.5.5.5\Pre-Requisites\SOLR Search Engine\solr\server\lib\ext\log4j-core-2.11.2.jar						
Installed version : 2.11.2						
Fixed version : 2.12.2						
Path : D:\EBS\New_CTS\Intalio Document - 11.5.5.5\Pre-Requisites\SOLR Search Engine\solr\contrib\prometheus-exporter\lib\log4j-core-2.11.2.jar						
Installed version : 2.11.2						
Fixed version : 2.12.2						
Path : D:\EBS\New_CTS\Intalio Document - 11.5.5.4\Pre-Requisites\SOLR Search Engine\solr\server\lib\ext\log4j-core-2.11.2.jar						
Installed version : 2.11.2						
Fixed version : 2.12.2						
Path : D:\EBS\New_CTS\Intalio Document - 11.5.5.4\Pre-Requisites\SOLR Search Engine\solr\contrib\prometheus-exporter\lib\log4j-core-2.11.2.jar						
Installed version : 2.11.2						
Fixed version : 2.12.2						
Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.						
Description: The version of Apache Log4j on the remote host is 2.x < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.						
Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.						
Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.						
Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.						
See Also: https://github.com/apache/logging-log4j2/pull/608 https://logging.apache.org/log4j/2.x/security.html						
Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
156002	Apache Log4j < 2.15.0 Remote Code Execution (Windows)	Misc.	Critical	10.2.42.120	TCP	445
MAC Address: 00:50:56:80:c0:ac						

DNS Name: adkdcvvpupsm1.ad.mohap.gov.ae

NetBIOS Name: ad.mohap.gov.ae\ADKDCVVPUPSM1

Plugin Output:

Plugin Output:

Path : D:\Vertiv_Critical_Insight\DB\XE\dbhomeXE\md\property_graph\pgx\server\pgx-webapp-2.5.1.war

Installed version : 2.9.0

Fixed version : 2.12.2

Path : D:\Vertiv_Critical_Insight\DB\XE\dbhomeXE\md\property_graph\pgx\server\pgx-webapp-2.5.1-wls.war

Installed version : 2.9.0

Fixed version : 2.12.2

Path : D:\Vertiv_Critical_Insight\DB\XE\dbhomeXE\md\property_graph\lib\log4j-core-2.9.0.jar

Installed version : 2.9.0

Fixed version : 2.12.2

Path : D:\Temp\DVD_VCI_61\Oracle\WINDOWS.X64_193000_db_home\md\property_graph\pgx\server\pgx-webapp-3.2.0.war

Installed version : 2.11.0

Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.35.53	TCP	0

MAC Address: 00:50:56:80:d4:0c

DNS Name: adkdcvvusmadb2.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /u01/grid/19c/tfa/adkdcvvusmadb2/tfa_home/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.100.31	TCP	0
MAC Address: 00:50:56:bb:f3:ce						
DNS Name: smartappstest2.moh.gov.ae						
NetBIOS Name:						
Plugin Output: Plugin Output: Path : /home/oracle/software/patches/Weblogic/31961038/files/oracle.log4j.log4j/1.2.17.0.0/thirdparty.symbol/modules/thirdparty/log4j-1.2.17.jar Installed version : 2.12.1 Fixed version : 2.12.2						
Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.						
Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.						
Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.						
Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.						
Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.						
See Also: https://github.com/apache/logging-log4j2/pull/608 https://logging.apache.org/log4j/2.x/security.html						

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.100.189	TCP	0
MAC Address: 00:50:56:80:2f:92						
DNS Name: adkdcvvdssfnt1.moh.ae						
NetBIOS Name:						
Plugin Output: Plugin Output: Path : /data/IBM/WebSphere/AppServer/properties/patches/backup/9.0.5.3-WS-WASProd-IFPH42728/systemApps/isclite.ear/kc.war/WEB-INF/lib/log4j-core-2.8.2.jar Installed version : 2.8.2 Fixed version : 2.12.2						
Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.						
Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.						
Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.						
Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.						

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.20.88	TCP	0

MAC Address: 00:50:56:bb:69:73

DNS Name: mh-kddb-pwsprd.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /data/app/oracle/product/12.2.0/db_1/md/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Path : /data/app/oracle/patch/33587128/files/md/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Path : /data/app/oracle/oradata/Patch/30886680/files/md/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Path : /data/Patches/July2021/32916808/files/md/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Path : /data/Patches/Jan2021/32228578/files/md/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Path : /data/Patches/31741641/files/md/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote	Misc.	Critical	10.2.46.145	TCP	0

Full Name: و.هبة.iraS
File Name: file'test.pdf
File Version: 1.11.0
Structure: Quality Assurance

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.20.21	TCP	0
MAC Address: 00:50:56:bb:b7:ea						
DNS Name: mhibmprdsr02.moh.ae						
NetBIOS Name:						
Plugin Output: Plugin Output: Path : /disk02/IBM/WebSphere/AppServer/systemApps/isclite.ear/kc.war/WEB-INF/lib/log4j-core-2.0.2.jar Installed version : 2.0.2 Fixed version : 2.3.1						
Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.						
Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.						
Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.						
Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.						
Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.						
See Also: https://github.com/apache/logging-log4j2/pull/608 https://logging.apache.org/log4j/2.x/security.html						

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.48.38	TCP	0
MAC Address: 00:50:56:bb:5e:68						
DNS Name: adkdcvvussdbr1						
NetBIOS Name:						
Plugin Output: Plugin Output: Path : /u01/oraclesoftware/suptools/tfa/release/tfa_home/jlib/log4j-core-2.9.1.jar Installed version : 2.9.1 Fixed version : 2.12.2 Path : /u01/oracle_software/Patch/GI/31305339/31281355/files/md/property_graph/lib/log4j-core-2.11.0.jar Installed version : 2.11.0 Fixed version : 2.12.2 Path : /u01/grid/19.3.0/tfa/adkdcvvussdbr1/tfa_home/jlib/log4j-core-2.9.1.jar Installed version : 2.9.1 Fixed version : 2.12.2						
Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.						
Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.						
Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.						

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.100.141	TCP	0

MAC Address: 00:50:56:bb:0f:db

DNS Name: adkdcvussptl1.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /data/Backup/IBM/WebSphere/AppServer/systemApps/isc-lite.ear/kc.war/WEB-INF/lib/log4j-core-2.0.2.jar

Installed version : 2.0.2

Fixed version : 2.3.1

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.41.197	TCP	0

MAC Address: 00:50:56:bc:8b:0d

DNS Name: mhinjomdbpm02.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /opt/ibm/ilog/doc/runtime/app/kc.war/WEB-INF/lib/log4j-core-2.0.2.jar

Installed version : 2.0.2

Fixed version : 2.3.1

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.40.168	TCP	0

MAC Address: 00:50:56:bb:f6:03

DNS Name: adkdcvvpwlsdb1.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /u01/app_ora/oracle/product/19.3/suptools/tfa/release/tfa_home/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Path : /u01/app_ora/oracle/product/19.3/md/property_graph/lib/log4j-core-2.11.0.jar

Installed version : 2.11.0

Fixed version : 2.12.2

Path : /u01/app_grid/grid/19.3/suptools/tfa/release/tfa_home/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.100.66	TCP	0

MAC Address: 00:50:56:bb:81:78

DNS Name: adkdcvdsstl1.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /data/Backup/IBM/WebSphere/AppServer/systemApps/isclite.ear/kc.war/WEB-INF/lib/log4j-core-2.0.2.jar

Installed version : 2.0.2

Fixed version : 2.3.1

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is $2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0$. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.100.12	TCP	0

MAC Address: 00:50:56:80:8b:f9

DNS Name: adkdcvuintgdb2.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /u01/grid/ora19c/tfa/adkdcvuintgdb2/tfa_home/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is $2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0$. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.20.87	TCP	0

MAC Address: 00:50:56:bb:5c:57

DNS Name: mh-kddb-nwsprd.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /u01/Patch/Oct/31667176/files/md/property_graph/lib/log4j-core-2.11.0.jar

Installed version : 2.11.0
Fixed version : 2.12.2

Path : /u01/Patch/Jan/32218454/files/md/property_graph/lib/log4j-core-2.11.0.jar
Installed version : 2.11.0
Fixed version : 2.12.2

Path : /u01/Patch/30869156/files/md/property_graph/lib/log4j-core-2.11.0.jar
Installed version : 2.11.0
Fixed version : 2.12.2

Path : /data/app/oracle/product/12.2.0/db_1/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /data/app/oracle/patch/33587128/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /data/app/oracle/oradata/Patch/30886680/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.20.92	TCP	0

MAC Address: 00:50:56:bb:e6:5a

DNS Name: adkdcvumohdb2.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /data/app/oracle/product/12.2.0/db_1/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /data/app/oracle/oradata/Patch/30886680/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /data/Patches/Oct2021/33261817/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /data/Patches/July2021/32916808/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1

Fixed version : 2.12.2

Path : /data/Patches/Jan2022/33587128/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /data/Patches/Jan2021/32228578/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /data/Patches/31741641/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is $2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0$. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.20.65	TCP	0

MAC Address: 00:50:56:80:b0:2b

DNS Name: adkdcvperpdb1.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /u04/oracle12/OHS12.2.1.4/oracle_common/modules/thirdparty/log4j-2.11.1.jar
Installed version : 2.11.1
Fixed version : 2.12.2

Path : /u04/oracle12/Middleware/Oracle_Home/oracle_common/modules/thirdparty/log4j-2.11.1.jar
Installed version : 2.11.1
Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is $2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0$. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.100.233	TCP	0
MAC Address: 00:50:56:bb:6d:13						
DNS Name: adkdcvussdb3.moh.ae						
NetBIOS Name:						
Plugin Output: Plugin Output: Path : /data/app/oracle/product/12.2.0/db_1/md/jlib/log4j-core-2.9.1.jar Installed version : 2.9.1 Fixed version : 2.12.2 Path : /data/app/oracle/oradata/Patch/30886680/files/md/jlib/log4j-core-2.9.1.jar Installed version : 2.9.1 Fixed version : 2.12.2 Path : /data/Patches/Oct2021/33261817/files/md/jlib/log4j-core-2.9.1.jar Installed version : 2.9.1 Fixed version : 2.12.2 Path : /data/Patches/July2021/32916808/files/md/jlib/log4j-core-2.9.1.jar Installed version : 2.9.1 Fixed version : 2.12.2 Path : /data/Patches/Jan2022/33587128/files/md/jlib/log4j-core-2.9.1.jar Installed version : 2.9.1 Fixed version : 2.12.2 Path : /data/Patches/Jan2021/32228578/files/md/jlib/log4j-core-2.9.1.jar Installed version : 2.9.1 Fixed version : 2.12.2 Path : /data/Patches/31741641/files/md/jlib/log4j-core-2.9.1.jar Installed version : 2.9.1 Fixed version : 2.12.2						
Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.						
Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands. Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled. Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.						
Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.						
See Also: https://github.com/apache/logging-log4j2/pull/608 https://logging.apache.org/log4j/2.x/security.html						

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.100.232	TCP	0

MAC Address: 00:50:56:bb:de:fd

DNS Name: adkdcvvusdb2.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /data/app/oracle/product/12.2.0/db_1/md/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Path : /data/app/oracle/oradata/Patch/30886680/files/md/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Path : /data/Patches/Oct2021/33261817/files/md/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Path : /data/Patches/July2021/32916808/files/md/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Path : /data/Patches/Jan2022/33587128/files/md/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Path : /data/Patches/Jan2021/32228578/files/md/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Path : /data/Patches/31741641/files/md/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>

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

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.100.190	TCP	0

MAC Address: 00:50:56:bb:53:dc

DNS Name: adkdcvvdssfdb4.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /data/app/oracle/product/12.2.0/db_1/md/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Path : /data/app/oracle/patch/33587128/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /data/app/oracle/oradata/Patch/30886680/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /data/Patches/Jan2022/33587128/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.42.27	TCP	0

MAC Address: 00:50:56:bb:1e:a1

DNS Name: mhibmprdsr06.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /disk02/IBM/WebSphere/AppServer/systemApps/isclite.ear/kc.war/WEB-INF/lib/log4j-core-2.0.2.jar
Installed version : 2.0.2
Fixed version : 2.3.1

Path : /data/IBM/WebSphere/AppServer/properties/patches/backup/9.0.5.3-WASProd-IFPH42728/systemApps/isclite.ear/kc.war/WEB-INF/lib/log4j-core-2.8.2.jar
Installed version : 2.8.2
Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.			TCP	0
MAC Address: 00:50:56:bb:89:a9						
DNS Name: adkdcvvdssbdb1.moh.ae						
NetBIOS Name:						
Plugin Output: Plugin Output: Path : /data/app/oracle/product/12.2.0/db_1/md/jlib/log4j-core-2.9.1.jar Installed version : 2.9.1 Fixed version : 2.12.2 Path : /data/app/oracle/patch/33587128/files/md/jlib/log4j-core-2.9.1.jar Installed version : 2.9.1 Fixed version : 2.12.2						
Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.						
Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands. Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled. Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.						
Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.						
See Also: https://github.com/apache/logging-log4j2/pull/608 https://logging.apache.org/log4j/2.x/security.html						

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.100.173	TCP	0
MAC Address: 00:50:56:bb:80:49						
DNS Name: mhbpmibmmhor01.moh.ae						
NetBIOS Name:						
Plugin Output: Plugin Output: Path : /data/app/oracle/product/12.2.0/db_1/md/jlib/log4j-core-2.9.1.jar Installed version : 2.9.1 Fixed version : 2.12.2 Path : /data/app/oracle/patch/33587128/files/md/jlib/log4j-core-2.9.1.jar Installed version : 2.9.1 Fixed version : 2.12.2						
Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.						
Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.						

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.42.86	TCP	0

MAC Address: 00:50:56:bb:10:60

DNS Name: adkdcvvpssdbr2

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /u01/grid/19.3.0/tfa/adkdcvvpssdbr2/tfa_home/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.100.231	TCP	0

MAC Address: 00:50:56:bb:91:4f

DNS Name: adkdcvussdb1.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /data/app/oracle/product/12.2.0/db_1/md/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.100.175	TCP	0

MAC Address: 00:50:56:80:b3:ef

DNS Name: mhbpmibmmhor03.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /data/app/oracle/product/12.2.0/db_1/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /data/app/oracle/patch/33587128/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /data/app/oracle/oradata/Patch/30886680/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /data/Patches/July2021/32916808/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /data/Patches/Jan2021/32228578/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /data/Patches/31741641/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.100.68	TCP	0
MAC Address: 00:50:56:bb:d6:de						
DNS Name: adkdcvvuintgdb1.moh.ae						
NetBIOS Name:						
Plugin Output: Plugin Output: Path : /data/ora19c/product/dbhome_1/suptools/tfa/release/tfa_home/jlib/log4j-core-2.9.1.jar Installed version : 2.9.1 Fixed version : 2.12.2 Path : /data/ora19c/product/dbhome_1/md/property_graph/lib/log4j-core-2.11.0.jar Installed version : 2.11.0 Fixed version : 2.12.2						
Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.						
Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands. Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled. Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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. See Also: https://github.com/apache/logging-log4j2/pull/608 https://logging.apache.org/log4j/2.x/security.html						

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.100.140	TCP	0
MAC Address: 00:50:56:bb:27:e6						
DNS Name: adkdcvvussbpm1.moh.ae						
NetBIOS Name:						
Plugin Output: Plugin Output: Path : /data/IBM/WebSphere/AppServer/profiles/BPMSTGNode1Profile/installedApps/mh-ibmstgwebCell02/IBM_BPM_KC_CI_BPMStgSingleCI.ear/KC_CI.war/WEB-INF/lib/log4j-core-2.8.2.jar Installed version : 2.8.2 Fixed version : 2.12.2						
Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.						
Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands. Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled. Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.100.187	TCP	0

MAC Address: 00:50:56:bb:88:99

DNS Name: adkdcvvdssbdb2.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /data/app/oracle/product/12.2.0/db_1/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /data/app/oracle/patch/33587128/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /data/app/oracle/oradata/Patch/30886680/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /data/Patches/Oct2021/33261817/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /data/Patches/July2021/32916808/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /data/Patches/Jan2022/33587128/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /data/Patches/Jan2021/32228578/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /data/Patches/31741641/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>

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

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.46.20	TCP	0
MAC Address: 00:50:56:bb:e9:89						
DNS Name: mhibmprdsr03.moh.ae						
NetBIOS Name:						
Plugin Output: Plugin Output: Path : /disk02/IBM/WebSphere/AppServer/profiles/MOHDmgrProfile/temp/wscache/installExtract/IBM_BPM_KC_CI_AppCluster.ear/KC_CI.war/ WEB-INF/lib/log4j-core-2.8.2.jar Installed version : 2.8.2 Fixed version : 2.12.2						
Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.						
Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.						
Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.						
Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.						
Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.						
See Also: https://github.com/apache/logging-log4j2/pull/608 https://logging.apache.org/log4j/2.x/security.html						

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.40.159	TCP	0
MAC Address: 00:50:56:bb:0a:94						
DNS Name: adkdcvvpwlsapp2.moh.ae						
NetBIOS Name:						
Plugin Output: Plugin Output: Path : /home/oracle/software/patches/Weblogic/31961038/files/oracle.log4j.log4j/1.2.17.0.0/thirdparty.symbol/modules/thirdparty/log4j-1.2.17.jar Installed version : 2.12.1 Fixed version : 2.12.2						
Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.						
Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.						
Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.						
Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.						
Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.100.116	TCP	0
MAC Address: 00:50:56:bb:7f:4d						
DNS Name: adkdcvussodm1.moh.ae						
NetBIOS Name:						
Plugin Output: Plugin Output: Path : /opt/ibm/ilog/doc/runtime/app/kc.war/WEB-INF/lib/log4j-core-2.0.2.jar Installed version : 2.0.2 Fixed version : 2.3.1						
Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.						
Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.						
Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.						
Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.						
Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.						
See Also: https://github.com/apache/logging-log4j2/pull/608 https://logging.apache.org/log4j/2.x/security.html						

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.42.85	TCP	0
MAC Address: 00:50:56:bb:53:89						
DNS Name: adkdcvvpssdbr1						
NetBIOS Name:						
Plugin Output: Plugin Output: Path : /u01/grid/19.3.0/tfa/adkdcvvpssdbr1/tfa_home/jlib/log4j-core-2.9.1.jar Installed version : 2.9.1 Fixed version : 2.12.2						
Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.						
Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.						
Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.						
Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.						
Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.20.91	TCP	0

MAC Address: 00:50:56:bb:aa:59

DNS Name: adkdcvumohdb1.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /data/app/oracle/product/12.2.0/db_1/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /data/Patches/Jan2022/33587128/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.100.142	TCP	0

MAC Address: 00:50:56:bb:1e:3b

DNS Name: adkdcvussfnt1.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /data01/IBM/WebSphere/AppServer/properties/patches/backup/9.0.5.3-WASProd-IFPH42728/systemApps/isclite.ear/kc.war/WEB-INF/lib/log4j-core-2.8.2.jar
Installed version : 2.8.2
Fixed version : 2.12.2

Path : /data/IBM/WebSphere/AppServer/properties/patches/backup/9.0.5.3-WASProd-IFPH42728/systemApps/isclite.ear/kc.war/WEB-INF/lib/log4j-core-2.8.2.jar
Installed version : 2.8.2
Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.41.196	TCP	0

MAC Address: 00:50:56:80:d0:a2

DNS Name: mhinjodmbpm01.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /opt/ibm/ilog/doc/runtime/app/kc.war/WEB-INF/lib/log4j-core-2.0.2.jar

Installed version : 2.0.2

Fixed version : 2.3.1

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.41.133	TCP	0

MAC Address: 00:50:56:bb:e0:02

DNS Name: mohkdcvlesbdev.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /soadata/Oracle/Middleware/Oracle_Home/oracle_common/modules/thirdparty/log4j-2.11.1.jar

Installed version : 2.11.1

Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is $2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0$. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.48.39	TCP	0

MAC Address: 00:50:56:bb:29:af

DNS Name: adkdcvvussdbr2

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /u01/oraclesoftware/suptools/tfa/release/tfa_home/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Path : /u01/oraclesoftware/md/property_graph/lib/log4j-core-2.11.0.jar

Installed version : 2.11.0

Fixed version : 2.12.2

Path : /u01/oraclesoftware/Patch/DB/31281355/files/md/property_graph/lib/log4j-core-2.11.0.jar

Installed version : 2.11.0

Fixed version : 2.12.2

Path : /u01/grid/19.3.0/tfa/adkdcvvussdbr2/tfa_home/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is $2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0$. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.40.158	TCP	0
MAC Address: 00:50:56:bb:97:f9						
DNS Name: smartappsnew1.moh.gov.ae						
NetBIOS Name:						
Plugin Output: Plugin Output: Path : /home/oracle/software/patches/Weblogic/31961038/files/oracle.log4j.log4j/1.2.17.0.0/thirdparty.symbol/modules/thirdparty/log4j-1.2.17.jar Installed version : 2.12.1 Fixed version : 2.12.2						
Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.						
Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.						
Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.						
Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.						
Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.						
See Also: https://github.com/apache/logging-log4j2/pull/608 https://logging.apache.org/log4j/2.x/security.html						

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.46.148	TCP	0
MAC Address: 00:50:56:bb:bb:ab						
DNS Name: adkdcvvpsoaosb2.moh.ae						
NetBIOS Name:						
Plugin Output: Plugin Output: Path : /soaosb/Oracle/Middleware/Oracle_Home/oracle_common/modules/thirdparty/log4j-2.11.1.jar Installed version : 2.11.1 Fixed version : 2.12.2						
Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.						
Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.						
Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.						
Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.						
Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.						
See Also: https://github.com/apache/logging-log4j2/pull/608						

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

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
--------	-------------	--------	----------	------------	----------	------

155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.100.174	TCP	0
--------	---	-------	----------	--------------	-----	---

MAC Address: 00:50:56:bb:0c:99

DNS Name: mhbpmibmmhor02.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /home/oracle/oracle.ahf/common/jlib/log4j-core-2.13.3.jar

Installed version : 2.13.3

Fixed version : 2.15.0

Path : /data/app/oracle/product/12.2.0/db_1/md/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Path : /data/app/oracle/patch/33587128/files/md/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>

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

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
--------	-------------	--------	----------	------------	----------	------

155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.42.20	TCP	0
--------	---	-------	----------	------------	-----	---

MAC Address: 00:50:56:bb:b7:1e

DNS Name: mhibmprdsr05.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /disk02/IBM/WebSphere/AppServer/systemApps/isclite.ear/kc.war/WEB-INF/lib/log4j-core-2.0.2.jar

Installed version : 2.0.2

Fixed version : 2.3.1

Path : /data/IBM/WebSphere/AppServer/properties/patches/backup/9.0.5.3-WASProd-IFPH42728/systemApps/isclite.ear/kc.war/WEB-INF/lib/log4j-core-2.8.2.jar

Installed version : 2.8.2

Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is $2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0$. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.100.102	TCP	0

MAC Address: 00:50:56:80:74:92

DNS Name: adkdcvvuintgdb3.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /u01/grid/ora19c/tfa/adkdcvvuintgdb3/tfa_home/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Path : /u01/dbhome/product/ora19c/db_1.0ld/suptools/tfa/release/tfa_home/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Path : /u01/dbhome/product/ora19c/db_1.0ld/md/property_graph/lib/log4j-core-2.11.0.jar

Installed version : 2.11.0

Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is $2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0$. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.46.149	TCP	0

MAC Address: 00:50:56:bb:bb:26

DNS Name: adkdcvvpsoaess1.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /soaosb/Oracle/Middleware/Oracle_Home/oracle_common/modules/thirdparty/log4j-2.11.1.jar

Installed version : 2.11.1

Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>

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

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.100.81	TCP	0

MAC Address: 00:50:56:bb:a3:17

DNS Name: adkdcvvuwsdb3.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /u01/app_grid/grid/19.3/tfa/adkdcvvuwsdb3/tfa_home/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>

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

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.41.201	TCP	0

MAC Address: 00:50:56:bb:16:98

DNS Name: adkdcvvpsoadbr2.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /u01/app/grid/tfa/adkdcvvpsoadbr2/tfa_home/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.46.150	TCP	0

MAC Address: 00:50:56:bb:f5:3a

DNS Name: adkdcvvpsoaess2.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /soaasb/Oracle/Middleware/Oracle_Home/oracle_common/modules/thirdparty/log4j-2.11.1.jar

Installed version : 2.11.1

Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote	Misc.	Critical	10.2.41.200	TCP	0

Code Execution
(Nix)

MAC Address: 00:50:56:bb:d4:41

DNS Name: adkdcvvpsoadbr1.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /u01/app/grid/tfa/adkdcvvpsoadbr1/tfa_home/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4.x < 2.12.3 / 2.13.x < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>

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

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.100.236	TCP	0

MAC Address: 00:50:56:bb:e6:2c

DNS Name: adkdcvvuwsdb1.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /u02/oracle19c/dbhome/product/19.3/suptools/tfa/release/tfa_home/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Path : /u02/oracle19c/dbhome/product/19.3/md/property_graph/lib/log4j-core-2.11.0.jar

Installed version : 2.11.0

Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4.x < 2.12.3 / 2.13.x < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>

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

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.20.89	TCP	0
MAC Address: 00:50:56:bb:54:c1						
DNS Name: mh-kddb-bpwwsr.moh.ae						
NetBIOS Name:						
Plugin Output: Plugin Output: Path : /data/app/oracle/product/12.2.0/db_1/md/jlib/log4j-core-2.9.1.jar Installed version : 2.9.1 Fixed version : 2.12.2 Path : /data/TFA_HOME/oracle.ahf/common/jlib/log4j-core-2.13.3.jar Installed version : 2.13.3 Fixed version : 2.15.0						
Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.						
Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands. Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled. Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.						
Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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. See Also: https://github.com/apache/logging-log4j2/pull/608 https://logging.apache.org/log4j/2.x/security.html						

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.46.146	TCP	0
MAC Address: 00:50:56:bb:12:4d						
DNS Name: adkdcvvpsoahp2.moh.ae						
NetBIOS Name:						
Plugin Output: Plugin Output: Path : /soahp/Oracle/Middleware/Oracle_Home/oracle_common/modules/thirdparty/log4j-2.11.1.jar Installed version : 2.11.1 Fixed version : 2.12.2						
Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.						
Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands. Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled. Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.						
Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.100.186	TCP	0

MAC Address: 00:50:56:bb:f9:11

DNS Name: adkdcvdsbpbdb2.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /patches/Patches/Oct2021/33261817/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /patches/Patches/July2021/32916808/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /patches/Patches/Jan2022/33587128/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /patches/Patches/Jan2021/32228578/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /patches/Patches/31741641/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /data/app/oracle/product/12.2.0/db_1/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.46.147	TCP	0

MAC Address: 00:50:56:bb:50:dd

DNS Name: adkdcvvpsoaosb1.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /soaosb/Oracle/Middleware/Oracle_Home/oracle_common/modules/thirdparty/log4j-2.11.1.jar

Installed version : 2.11.1

Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is $2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0$. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.100.11	TCP	0

MAC Address: 00:50:56:bb:a5:2c

DNS Name: adkdcvvuwlisapp1.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /u01/OracleSoftware/patches/Weblogic/31961038/files/oracle.log4j.log4j/1.2.17.0.0/thirdparty.symbol/modules/thirdparty/log4j-1.2.17.jar

Installed version : 2.12.1

Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is $2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0$. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote	Misc.	Critical	10.2.100.10	TCP	0

Code Execution (Nix)

MAC Address: 00:50:56:bb:56:5a

DNS Name: adkdcvuwlsdb2.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /u01/app_grid/grid/19.3/tfa/adkdcvuwlsdb2/tfa_home/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>

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

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.20.94	TCP	0

MAC Address: 00:50:56:bb:4e:34

DNS Name: adkdcvvdssbdb3.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /data/app/oracle/product/12.2.0/db_1/md/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Path : /data/app/oracle/patch/33587128/files/md/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Path : /data/app/oracle/oradata/Patch/30886680/files/md/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Path : /data/Patches/Oct2021/33261817/files/md/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Path : /data/Patches/July2021/32916808/files/md/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Path : /data/Patches/Jan2022/33587128/files/md/jlib/log4j-core-2.9.1.jar

Installed version : 2.9.1

Fixed version : 2.12.2

Path : /data/Patches/Jan2021/32228578/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Path : /data/Patches/31741641/files/md/jlib/log4j-core-2.9.1.jar
Installed version : 2.9.1
Fixed version : 2.12.2

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port
--------	-------------	--------	----------	------------	----------	------

155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)	Misc.	Critical	10.2.20.20	TCP	0
--------	---	-------	----------	------------	-----	---

MAC Address: 00:50:56:bb:0a:e8

DNS Name: mhibmprdsr01.moh.ae

NetBIOS Name:

Plugin Output:

Plugin Output:

Path : /disk02/IBM/WebSphere/AppServer/systemApps/islite.ear/kc.war/WEB-INF/lib/log4j-core-2.0.2.jar
Installed version : 2.0.2
Fixed version : 2.3.1

Synopsis: A package installed on the remote host is affected by a remote code execution vulnerability.

Description: The version of Apache Log4j on the remote host is 2.x < 2.3.1 / 2.4 < 2.12.3 / 2.13 < 2.15.0. It is, therefore, affected by a remote code execution vulnerability in the JNDI parser due to improper log validation. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.

Log4j 1.x, which reached its End of Life prior to 2016, comes with JMSAppender which will perform a JNDI lookup if enabled in Log4j's configuration file, hence customers should evaluate triggers in 1.x based on the risk that it is EOL and whether JNDI lookups are enabled.

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution: Upgrade to Apache Log4j version 2.3.1 / 2.12.3 / 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.

See Also: <https://github.com/apache/logging-log4j2/pull/608>
<https://logging.apache.org/log4j/2.x/security.html>