An official website of the United States government Here's how you know

NVD

VULNERABILITIES

CVE-2021-45046 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. This could allows attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, $${ctx:loginId}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern resulting in a denial of service (DOS) attack. Log4j 2.15.0 makes a best-effort attempt to restrict JNDI LDAP lookups to localhost by default. Log4j 2.16.0 fixes this issue by removing support for message lookup patterns and disabling JNDI functionality by default.

+View Analysis Description

Severity

CVSS Version 3.x	CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD

Base Score: 3.7 LOW

Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
http://www.openwall.com/lists/oss-security/2021/12/14/4	**Mailing List** **Mitigation** **Third Party Advisory**
http://www.openwall.com/lists/oss-security/2021/12/15/3	
https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf	
https://logging.apache.org/log4j/2.x/security.html	**Mitigation** **Release Notes** **Vendor Advisory**
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd	
https://www.cve.org/CVERecord?id=CVE-2021-44228	**Not Applicable**
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00646.html	**Third Party Advisory**
https://www.kb.cert.org/vuls/id/930724	

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-502	Deserialization of Untrusted Data	NIST Apache Software Foundation

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:a:apache:log4j:2.0:-:*:*:*:*:*:* Show Matching CPE(s)		
cpe:2.3:a:apache:log4j:2.0:beta9:*:*:*:*:*:* Show Matching CPE(s)		
cpe:2.3:a:apache:log4j:2.0:rc1:*:*:*:*:*:* Show Matching CPE(s)		
cpe:2.3:a:apache:log4j:2.0:rc2:*:*:*:*:*:* Show Matching CPE(s)		
cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:* Show Matching CPE(s)	**From (including) 2.0.1**	**Up to (including) 2.12.1**
cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:* Show Matching CPE(s)	**From (including) 2.13.0**	**Up to (excluding) 2.15.0**

Configuration 2 (hide)

cpe:2.3:a:intel:audio_development_kit:-:*:*:*:*:*:*:* Show Matching CPE(s)
cpe:2.3:a:intel:datacenter_manager:-:*:*:*:*:*:*:* Show Matching CPE(s)
cpe:2.3:a:intel:oneapi:-:*:*:*:*:eclipse:*:* Show Matching CPE(s)
cpe:2.3:a:intel:secure_device_onboard:-:*:*:*:*:*:*:* Show Matching CPE(s)
cpe:2.3:a:intel:system_debugger:-:*:*:*:*:*:*:* Show Matching CPE(s)

Configuration 3 (hide)

cpe:2.3:a:netapp:brocade_san_navigator:-:*:*:*:*:*:*:* Show Matching CPE(s)
cpe:2.3:a:netapp:cloud_insights_acquisition_unit:-:*:*:*:*:*:*:* Show Matching CPE(s)

cpe:2.3:a:netapp:cloud_manager:-:*:*:*:*:*:*:*

Show Matching CPE(s)

cpe:2.3:a:netapp:cloud_secure_agent:-:*:*:*:*:*:*:*

Show Matching CPE(s)

cpe:2.3:a:netapp:oncommand_insight:-:*:*:*:*:*:*:*

Show Matching CPE(s)

cpe:2.3:a:netapp:ontap_tools:-:*:*:*:*:vmware_vsphere:*:*

Show Matching CPE(s)

cpe:2.3:a:netapp:snapcenter:-:*:*:*:*:vmware_vsphere:*:*

Show Matching CPE(s)

Configuration 4 (hide)

cpe:2.3:o:fedoraproject:fedora:35:*:*:*:*:*:*:*

Show Matching CPE(s)

Configuration 5 (hide)

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*

Show Matching CPE(s)

cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:*:*

Show Matching CPE(s)

cpe:2.3:o:debian:debian_linux:11.0:*:*:*:*:*:*:*

Show Matching CPE(s)

Configuration 6 (hide)

cpe:2.3:a:arubanetworks:silver_peak_orchestrator:-:*:*:*:*:*:*:*

Show Matching CPE(s)

Configuration 7 (hide)

cpe:2.3:a:siemens:capital:-:*:*:*:*:*:*:*

Show Matching CPE(s)

cpe:2.3:a:siemens:cosmos:-:*:*:*:*:*:*:*

Show Matching CPE(s)

cpe:2.3:a:siemens:desigo_consumption_control_advanced_reporting:*:*:*:*:*:*:*:*

Show Matching CPE(s)

cpe:2.3:a:siemens:desigo_consumption_control_advanced_reporting:-:*:*:*:*:*:*:*

Show Matching CPE(s)

cpe:2.3:a:siemens:desigo_consumption_control_advanced_reporting:4.0:*:*:*:*:*:*:*

Show Matching CPE(s)

cpe:2.3:a:siemens:desigo_consumption_control_advanced_reporting:4.1:*:*:*:*:*:*:* Show Matching CPE(s)		
cpe:2.3:a:siemens:desigo_consumption_control_advanced_reporting:4.2:*:*:*:*:*:*:* Show Matching CPE(s)		
cpe:2.3:a:siemens:desigo_consumption_control_advanced_reporting:5.0:*:*:*:*:*:*:* Show Matching CPE(s)		
cpe:2.3:a:siemens:desigo_consumption_control_advanced_reporting:5.1:*:*:*:*:*:*:* Show Matching CPE(s)		
cpe:2.3:a:siemens:desigo_consumption_control_info_center:5.0:*:*:*:*:*:*:* Show Matching CPE(s)		
cpe:2.3:a:siemens:desigo_consumption_control_info_center:5.1:*:*:*:*:*:*:* Show Matching CPE(s)		
cpe:2.3:a:siemens:e-car_operating_center:*:*:*:*:cloud:*:*:* Show Matching CPE(s)	Up to (excluding) 2021-12-13	
cpe:2.3:a:siemens:energyip_prepay:3.7:*:*:*:*:*:*:* Show Matching CPE(s)		
cpe:2.3:a:siemens:energyip_prepay:3.8:*:*:*:*:*:*:* Show Matching CPE(s)		
cpe:2.3:a:siemens:gma-manager:*:*:*:*:*:*:*:* Show Matching CPE(s)	From (including) 8.6.2j-398	
cpe:2.3:a:siemens:head-end_system_universal_device_integration_system:-:*:*:*:*:*:*:* Show Matching CPE(s)		
cpe:2.3:a:siemens:industrial_edge_management:-:*:*:*:*:*:*:* Show Matching CPE(s)		
cpe:2.3:a:siemens:simatic_wincc:7.4:*:*:*:*:*:*:* Show Matching CPE(s)		
cpe:2.3:a:siemens:sipass_integrated:2.80:*:*:*:*:*:*:* Show Matching CPE(s)		
cpe:2.3:a:siemens:sipass_integrated:2.85:*:*:*:*:*:*:* Show Matching CPE(s)		
cpe:2.3:a:siemens:siveillance_command:*:*:*:*:*:*:*:* Show Matching CPE(s)	Up to (including) 4.16.2.1	
cpe:2.3:a:siemens:siveillance_control:*:*:*:*:pro:*:*:* Show Matching CPE(s)	Up to (excluding) 2.1	

cpe:2.3:a:siemens:siveillance_identity:1.5:*:*:*:*:*:*:*		
Show Matching CPE(s)		
cpe:2.3:a:siemens:siveillance_identity:1.6:*:*:*:*:*:*:*		
Show Matching CPE(s)		
cpe:2.3:a:siemens:siveillance_vantage:-:*:*:*:*:*:*:*		
Show Matching CPE(s)		
cpe:2.3:a:siemens:solid_edge_wiring_harness_design:-:*:*:*:*:*:*:*		
Show Matching CPE(s)		
cpe:2.3:a:siemens:spectrum_power_4:*:*:*:*:*:*:*:*	Up to (excluding) 4.70	
Show Matching CPE(s)		
cpe:2.3:a:siemens:spectrum_power_4:4.70:-:*:*:*:*:*:*		
Show Matching CPE(s)		
cpe:2.3:a:siemens:spectrum_power_4:4.70:sp7:*:*:*:*:*:*		
Show Matching CPE(s)		
cpe:2.3:a:siemens:spectrum_power_4:4.70:sp8:*:*:*:*:*:*		
Show Matching CPE(s)		
cpe:2.3:a:siemens:spectrum_power_7:-:*:*:*:*:*:*:*		
Show Matching CPE(s)		
cpe:2.3:a:siemens:teamcenter_suite:-:*:*:*:*:*:*:*		
Show Matching CPE(s)		
cpe:2.3:a:siemens:vesys:-:*:*:*:*:*:*:*		
Show Matching CPE(s)		
cpe:2.3:a:siemens:xpedition_enterprise_data_management:*:*:*:*:*:*:*:*	From (including) 2.6	Up to (including) 2.10
Show Matching CPE(s)		
cpe:2.3:a:siemens:xpedition_package_integrator:*:*:*:*:*:*:*:*	From (including) 2.6	Up to (including) 2.10
Show Matching CPE(s)		
cpe:2.3:o:siemens:dynamic_security_assessment:4.2:*:*:*:*:*:*:*		
Show Matching CPE(s)		
cpe:2.3:o:siemens:dynamic_security_assessment:4.3:*:*:*:*:*:*:*		
Show Matching CPE(s)		
cpe:2.3:o:siemens:dynamic_security_assessment:4.4:*:*:*:*:*:*:*		
Show Matching CPE(s)		
cpe:2.3:o:siemens:industrial_edge_management:-:*:*:*:*:*:*:*		
Show Matching CPE(s)		
cpe:2.3:o:siemens:industrial_edge_manangement_hub:-:*:*:*:*:*:*:*		
Show Matching CPE(s)		

cpe:2.3:o:siemens:logo\!_soft_comfort:-:*:*:*:*:*:*:* Show Matching CPE(s)	
cpe:2.3:o:siemens:mendix:-:*:*:*:*:*:*:* Show Matching CPE(s)	
cpe:2.3:o:siemens:mindsphere:*:*:*:*:cloud:*:*:* Show Matching CPE(s)	Up to (excluding) 2021-12-11
cpe:2.3:o:siemens:nx:-:*:*:*:*:*:*:* Show Matching CPE(s)	
cpe:2.3:o:siemens:opcenter_intelligence:*:*:*:*:*:*:*:* Show Matching CPE(s)	From (including) 3.2
cpe:2.3:o:siemens:operation_scheduler:*:*:*:*:*:*:*:* Show Matching CPE(s)	From (including) 1.1.3

Denotes Vulnerable Software

Are we missing a CPE here? Please let us know.

Change History

8 change records found show changes

QUICK INFO

CVE Dictionary Entry:

CVE-2021-45046

NVD Published Date:

12/14/2021

NVD Last Modified:

12/16/2021

Source:

Apache Software Foundation

HEADQUARTERS
100 Bureau Drive
Gaithersburg, MD 20899
(301) 975-2000

Incident Response Assistance and Non-NVD Related Technical Cyber Security Questions:
US-CERT Security Operations Center
Email: soc@us-cert.gov
Phone: 1-888-282-0870
Sponsored by
CISA