CISA Log4j (CVE-2021-44228) Affected Vendor & Software List

Status Descriptions

Status	Description
Unknown	Status unknown. Default choice.
Affected	Reported to be affected by CVE-2021-44228.
Not Affected	Reported to NOT be affected by CVE-2021-44228 and no further action necessary.
Fixed	Patch and/or mitigations available (see provided links).
Under Investigation	Vendor investigating status.

Software List

This list was initially populated using information from the following sources:

- Kevin Beaumont
- SwitHak

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
1Password	All products		Not affected		1Password statement			12/23/2021
2n					2n Advisory Link			
3CX					3CX Community Thread Link			
3M Health Information Systems	CGS		Affected	Unknown	CGS: Log4j Software Update(login required)	This advisory is available to customer only and has not been reviewed by CISA.		12/15/2021
7-Zip					7Zip Discussion Link			
ABB					ABB Link			
ABB	ABB Remote Service	ABB Remote Platform (RAP)	Affected		Details are shared with active subscribers			
ABB	AlarmInsight Cloud	AlarmInsight KPI Dashboards 1.0.0	Under Investigation					
ABB	B&R Products	See Vendor Advisory			BR-Automation Advisory			
Abbott					Abbott Advisory Link			12/15/2021
Abnormal Security	Abnormal Security		Not affected		Abnormal Blog			
Accellence					Accellence Article			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Accellion	Kiteworks	v7.6 release	Fixed	Yes	Kiteworks Statement	“As a precaution, Kiteworks released a 7.6.1 Hotfix software update to address the vulnerability. This patch release adds the mitigation for CVE-2021-44228 contained in the Solr package as recommended by Apache Solr group. Specifically, it updates the Log4j library to a non-vulnerable version on CentOS 7 systems as well as adds the recommended option “$SOLR_OPTS -Dlog4j2.formatMsgNoLookups=true” to disable the possible attack vector on both CentOS 6 and CentOS 7."		12/16/2021
Acquia					Acquia Article			
Acronis					Acronis Advisory Link			
ActiveState					ActiveState Blog Post			
Adaptec					Adaptec Link			
Addigy					Addigy Blog Post			
Adeptia					Adeptia Article			
Adobe ColdFusion					Adobe ColdFusion Link			
ADP					ADP Alert Link			
AFAS Software					AFAS Software Link			
AFHCAN Global LLC	AFHCANsuite	8.0.7 - 8.4.3	Not Affected		https://afhcan.org/support.aspx			
AFHCAN Global LLC	AFHCANServer	8.0.7 - 8.4.3	Not Affected		https://afhcan.org/support.aspx			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
AFHCAN Global LLC	AFHCANcart	8.0.7 - 8.4.3	Not Affected		https://afhcan.org/support.aspx			
AFHCAN Global LLC	AFHCANweb	8.0.7 - 8.4.3	Not Affected		https://afhcan.org/support.aspx			
AFHCAN Global LLC	AFHCANmobile	8.0.7 - 8.4.3	Not Affected		https://afhcan.org/support.aspx			
AFHCAN Global LLC	AFHCANupdate	8.0.7 - 8.4.3	Not Affected		https://afhcan.org/support.aspx			
Agilysys					Agilysys Link			
Advanced Systems Concepts (formally Jscape)	Active MFT		Not Affected	No	Log4J Vulnerabilty	This advisory is available to customers only and has not been reviewed by CISA		12/14/2021
Advanced Systems Concepts (formally Jscape)	MFT Server		Not Affected	No	Log4J Vulnerabilty	This advisory is available to customers only and has not been reviewed by CISA		12/14/2021
Advanced Systems Concepts (formally Jscape)	MFT Gateway		Not Affected	No	Log4J Vulnerabilty	This advisory is available to customers only and has not been reviewed by CISA		12/14/2021
Advanced Systems Concepts (formally Jscape)	MFT		Not Affected	No	Log4J Vulnerabilty	This advisory is available to customers only and has not been reviewed by CISA		12/14/2021
Akamai	SIEM Splunk Connector	All	Affected	Yes	Akamai SIEM Integration	v1.4.11 is the new recommendation for mitigation of log4j vulnerabilities		12/15/2021
Alcatel					Alcatel Link			
Alertus					Alertus Article Link			
Alexion					Alexion Blog Post			
Alfresco					Alfresco Blog Post			
AlienVault					AlienVault Article Link			
Alphatron Medical					Alphatron Medical Website			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Amazon	AWS	Linux 1,2	Not Affected	No		Notes: Amazon Linux 1 had aws apitools which were Java based but these were deprecated in 2015 AWS Forum. AMIs used to inspect and verify (base spin ups) - amzn-ami-hvm-2018.03.0.20200318.1-x86_64-gp2 and amzn2-ami-kernel-5.10-hvm-2.0.20211201.0-x86_64-gp2		12/15/2021
Amazon	AWS API Gateway	All	Fixed		Amazon AWS Link			12/20/2021
Amazon	AWS CloudHSM	< 3.4.1.	Affected		Apache Log4j2 Security Bulletin (CVE-2021-44228) (amazon.com)			
Amazon	AWS Connect	All	Fixed		Vendor Link	Vendors recommend evaluating components of the environment outside of the Amazon Connect service boundary, which may require separate/additional customer mitigation		12/23/2021
Amazon	AWS Lambda	Unknown	Affected	Yes	Apache Log4j2 Security Bulletin (CVE-2021-44228) (amazon.com)			
Amazon	EC2	Amazon Linux 1 & 2	Not Affected		Apache Log4j2 Security Bulletin (CVE-2021-44228) (amazon.com)			12/15/2021
Amazon	AWS DynamoDB	Unknown	Fixed		Update for Apache Log4j2 Issue (CVE-2021-44228)			12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Amazon	AWS ElastiCache	Unknown	Fixed		Update for Apache Log4j2 Issue (CVE-2021-44228)			12/17/2021
Amazon	AWS Inspector	Unknown	Fixed		Update for Apache Log4j2 Issue (CVE-2021-44228)			12/17/2021
Amazon	AWS RDS	Unknown	Fixed		Update for Apache Log4j2 Issue (CVE-2021-44228)	Amazon RDS and Amazon Aurora have been updated to mitigate the issues identified in CVE-2021-44228		12/17/2021
Amazon	AWS S3	Unknown	Fixed		Update for Apache Log4j2 Issue (CVE-2021-44228)			12/14/2021
Amazon	AWS SNS	Unknown	Fixed		Update for Apache Log4j2 Issue (CVE-2021-44228)	Amazon SNS systems that serve customer traffic are patched against the Log4j2 issue. We are working to apply the Log4j2 patch to sub-systems that operate separately from SNS's systems that serve customer traffic		12/14/2021
Amazon	AWS SQS	Unknown	Fixed		Update for Apache Log4j2 Issue (CVE-2021-44228)			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Amazon	AWS EKS, ECS, Fargate	Unknown	Affected	Yes	Update for Apache Log4j2 Issue (CVE-2021-44228)	To help mitigate the impact of the open-source Apache “Log4j2” utility (CVE-2021-44228 and CVE-2021-45046) security issues on customers’ containers, Amazon EKS, Amazon ECS, and AWS Fargate are deploying a Linux-based update (hot-patch). This hot-patch will require customer opt-in to use, and disables JNDI lookups from the Log4J2 library in customers’ containers. These updates are available as an Amazon Linux package for Amazon ECS customers, as a DaemonSet for Kubernetes users on AWS, and will be in supported AWS Fargate platform versions		12/16/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Amazon	AWS ELB	Unknown	Fixed		Update for Apache Log4j2 Issue (CVE-2021-44228)			12/16/2021
Amazon	AWS Kinesis Data Stream	Unknown	Affected	Yes	Update for Apache Log4j2 Issue (CVE-2021-44228)	We are actively patching all subsystems that use Log4j2 by applying updates. The Kinesis Client Library (KCL) version 2.X and the Kinesis Producer Library (KPL) are not impacted. For customers using KCL 1.x, we have released an updated version and we strongly recommend that all KCL version 1.x customers upgrade to KCL version 1.14.5 (or higher)		12/14/2021
Amazon	OpenSearch	Unknown	Affected	Yes	Apache Log4j2 Security Bulletin (CVE-2021-44228) (amazon.com), (R20211203-P2)			
Amazon	Translate		Not affected		Amazon Translate	Service not identified on AWS Log4j Security Bulletin		
AMD	All		Not Affected		AMD Advisory Link	Currently, no AMD products have been identified as affected. AMD is continuing its analysis.		12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Anaconda	Anaconda	4.10.3	Not Affected		https://docs.conda.io/projects/conda/en/latest/index.html			12/21/2021
Apache	ActiveMQ Artemis	All	Not Affected	Yes	ApacheMQ - Update on CVE-2021-4428	ActiveMQ Artemis does not use Log4j for logging. However, Log4j 1.2.17 is included in the Hawtio-based web console application archive (i.e. web/console.war/WEB-INF/lib). Although this version of Log4j is not impacted by CVE-2021-44228 future versions of Artemis will be updated so that the Log4j jar is no longer included in the web console application archive. See ARTEMIS-3612 for more information on that task.		12/21/2021
Apache	Airflow		Not affected		Apache Airflow	Airflow is written in Python		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Apache	Camel	3.14.1.3.11.5,3.7.7	Affected	Yes	APACHE CAMEL AND CVE-2021-44228 (LOG4J)	Apache Camel does not directly depend on Log4j 2, so we are not affected by CVE-2021-44228.If you explicitly added the Log4j 2 dependency to your own applications, make sure to upgrade.Apache Camel does use log4j during testing itself, and therefore you can find that we have been using log4j v2.13.3 release in our latest LTS releases Camel 3.7.6, 3.11.4.		12/13/2021
Apache	Camel Quarkus		Not Affected	No	APACHE CAMEL AND CVE-2021-44228 (LOG4J)			12/13/2021
Apache	Camel K		Not Affected	No	APACHE CAMEL AND CVE-2021-44228 (LOG4J)			12/13/2021
Apache	CamelKafka Connector		Not Affected	No	APACHE CAMEL AND CVE-2021-44228 (LOG4J)			12/13/2021
Apache	Camel Karaf		Affected	No	APACHE CAMEL AND CVE-2021-44228 (LOG4J)	The Karaf team is aware of this and are working on a new Karaf 4.3.4 release with updated log4j.		12/13/2021
Apache	Camel JBang	<=3.1.4	Affected	No	APACHE CAMEL AND CVE-2021-44228 (LOG4J)			12/13/2021
Apache	Camel 2		Not Affected	None	APACHE CAMEL AND CVE-2021-44228 (LOG4J)			12/13/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Apache	Druid	< druid 0.22.0	Affected	Yes	Release druid-0.22.1 · apache/druid · GitHub			12/12/2021
Apache	Flink	< 1.14.2, 1.13.5, 1.12.7, 1.11.6	Fixed	Yes	Apache Flink: Advise on Apache Log4j Zero Day (CVE-2021-44228)	To clarify and avoid confusion: The 1.14.1 / 1.13.4 / 1.12.6 / 1.11.5 releases, which were supposed to only contain a Log4j upgrade to 2.15.0, were skipped because CVE-2021-45046 was discovered during the release publication. The new 1.14.2 / 1.13.5 / 1.12.7 / 1.11.6 releases include a version upgrade for Log4j to version 2.16.0 to address CVE-2021-44228 and CVE-2021-45046.	https://flink.apache.org/news/2021/12/16/log4j-patch-releases.html	12/12/2021
Apache	Kafka	All	Not Affected	No	Kafka Apache List	The current DB lists Apache Kafka as impacted. Apache Kafka uses Log4jv1, not v2.		12/14/2021
Apache	Kafka	Unknown	Affected	No	Log4j – Apache Log4j Security Vulnerabilities	Only vulnerable in certain configuration(s)		
Apache	Log4j	< 2.15.0	Affected	Yes	Log4j – Apache Log4j Security Vulnerabilities			
Apache	Solr	7.4.0 to 7.7.3, 8.0.0 to 8.11.0	Fixed	Yes	Apache Solr Security	Update to 8.11.1 or apply fixes as described in Solr security advisory	Apache Solr 8.11.1 downloads	12/16/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Apache	Struts 2	Versions before 2.5.28.1	Fixed (See Notes)	Yes	Apache Struts Announcements	The Apache Struts group is pleased to announce that Struts 2.5.28.1 is available as a “General Availability” release. The GA designation is our highest quality grade. This release addresses Log4j vulnerability CVE-2021-45046 by using the latest Log4j 2.12.2 version (Java 1.7 compatible).	Apache Struts Release Downloads	12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Apache	Tomcat	9.0.x	Not Affected (See Notes)		Apache Tomcat Security Notes	Apache Tomcat 9.0.x has no dependency on any version of log4j. Web applications deployed on Apache Tomcat may have a dependency on log4j. You should seek support from the application vendor in this instance. It is possible to configure Apache Tomcat 9.0.x to use log4j 2.x for Tomcat's internal logging. This requires explicit configuration and the addition of the log4j 2.x library. Anyone who has switched Tomcat's internal logging to log4j 2.x is likely to need to address this vulnerability. In most cases, disabling the problematic feature will be the simplest solution. Exactly how to do that depends on the exact version of log4j 2.x being used. Details are provided on the log4j 2.x security page		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Apereo	CAS	6.3.x & 6.4.x	Affected	Yes	CAS Log4J Vulnerability Disclosure – Apereo Community Blog			
Apereo	Opencast	< 9.10, < 10.6	Affected	Yes	Apache Log4j Remote Code Execution · Advisory · opencast/opencast · GitHub			
Application Performance Ltd	DBMarlin	Not Affected		Common Vulnerabilities Apache log4j Vulnerability CVE-2021-4428				12/15/2021
Apigee					Apigee Link			
Apollo					Apollo Community Link			
Appdynamics					Appdynamics Advisory Link			
Appeon	PowerBuilder	Appeon PowerBuilder 2017-2021 regardless of product edition	Affected	No				12/15/2021
AppGate					AppGate Blog Post			
Appian	Appian Platform	All	Fixed		KB-2204 Information about the Log4j2 security vulnerabilities (CVE-2021-44228 & CVE-2021-45046)			12/22/2021
Application Performance Ltd	DBMarlin		Not Affected		Common Vulnerabilities Apache log4j Vulnerability CVE-2021-4428			12/15/2021
APPSHEET					APPSHEET Community Link			
Aptible	Aptible	ElasticSearch 5.x	Affected	Yes	Aptible Status - Log4j security incident CVE-2021-27135			
APC by Schneider Electric	Powerchute Business Edition	v9.5, v10.0.1, v10.0.2, v10.0.3, v10.0.4	Fixed	No	https://community.exchange.se.com/t5/APC-UPS-Data-Center-Backup/Log4-versions-used-in-Powerchute-vulnerable/m-p/379866/highlight/true#M47345	Mitigation instructions to remove the affected class.		12/15/2021
APC by Schneider Electric	Powerchute Network Shutdown	4.2, 4.3, 4.4, 4.4.1	Fixed	No	https://community.exchange.se.com/t5/APC-UPS-Data-Center-Backup/Log4-versions-used-in-Powerchute-vulnerable/m-p/379866/highlight/true#M47345	Mitigation instructions to remove the affected class.		12/15/2021
Aqua Security					Aqua Security Google Doc			
Arbiter Systems	All		Not Affected		Arbiter Systems Advisory Link			12/22/2021
Arca Noae					Arca Noae Link			
Arcserve	Arcserve Backup	All	Not Affected	No	https://support.storagecraft.com/s/article/Log4J-Update		https://support.storagecraft.com/s/question/0D51R000089NnT3SAK/does-storagecraft-have-a-publicly-available-response-to-the-log4j-vulnerability-is-there-a-reference-for-any-findings-negative-positive-the-company-has-in-their-investigations-it-seems-it-would-greatly-benefit-support-and-customers-both?language=en_US	12/14/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Arcserve	Arcserve Continuous Availability	All	Not Affected	No	https://support.storagecraft.com/s/article/Log4J-Update		https://support.storagecraft.com/s/question/0D51R000089NnT3SAK/does-storagecraft-have-a-publicly-available-response-to-the-log4j-vulnerability-is-there-a-reference-for-any-findings-negative-positive-the-company-has-in-their-investigations-it-seems-it-would-greatly-benefit-support-and-customers-both?language=en_US	12/14/2021
Arcserve	Arcserve Email Archiving	All	Not Affected	No	https://support.storagecraft.com/s/article/Log4J-Update		https://support.storagecraft.com/s/question/0D51R000089NnT3SAK/does-storagecraft-have-a-publicly-available-response-to-the-log4j-vulnerability-is-there-a-reference-for-any-findings-negative-positive-the-company-has-in-their-investigations-it-seems-it-would-greatly-benefit-support-and-customers-both?language=en_US	12/14/2021
Arcserve	Arcserve UDP	6.5-8.3	Not Affected	No	https://support.storagecraft.com/s/article/Log4J-Update		https://support.storagecraft.com/s/question/0D51R000089NnT3SAK/does-storagecraft-have-a-publicly-available-response-to-the-log4j-vulnerability-is-there-a-reference-for-any-findings-negative-positive-the-company-has-in-their-investigations-it-seems-it-would-greatly-benefit-support-and-customers-both?language=en_US	12/14/2021
Arcserve	ShadowProtect	All	Not Affected	No	https://support.storagecraft.com/s/article/Log4J-Update		https://support.storagecraft.com/s/question/0D51R000089NnT3SAK/does-storagecraft-have-a-publicly-available-response-to-the-log4j-vulnerability-is-there-a-reference-for-any-findings-negative-positive-the-company-has-in-their-investigations-it-seems-it-would-greatly-benefit-support-and-customers-both?language=en_US	12/14/2021
Arcserve	ShadowXafe	All	Not Affected	No	https://support.storagecraft.com/s/article/Log4J-Update		https://support.storagecraft.com/s/question/0D51R000089NnT3SAK/does-storagecraft-have-a-publicly-available-response-to-the-log4j-vulnerability-is-there-a-reference-for-any-findings-negative-positive-the-company-has-in-their-investigations-it-seems-it-would-greatly-benefit-support-and-customers-both?language=en_US	12/14/2021
Arcserve	Solo	All	Not Affected	No	https://support.storagecraft.com/s/article/Log4J-Update		https://support.storagecraft.com/s/question/0D51R000089NnT3SAK/does-storagecraft-have-a-publicly-available-response-to-the-log4j-vulnerability-is-there-a-reference-for-any-findings-negative-positive-the-company-has-in-their-investigations-it-seems-it-would-greatly-benefit-support-and-customers-both?language=en_US	12/14/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Arcserve	StorageCraft OneXafe	All	Not Affected	No	https://support.storagecraft.com/s/article/Log4J-Update		https://support.storagecraft.com/s/question/0D51R000089NnT3SAK/does-storagecraft-have-a-publicly-available-response-to-the-log4j-vulnerability-is-there-a-reference-for-any-findings-negative-positive-the-company-has-in-their-investigations-it-seems-it-would-greatly-benefit-support-and-customers-both?language=en_US	12/14/2021
ArcticWolf					ArcticWolf Blog Post			
Arduino					Arduino Support Link			
Ariba					Ariba Annoucement			
Arista					Arista Advisory Notice			
Aruba Networks					Aruba Networks Notification			
Ataccama					Ataccama Link			
Atera					Atera Link			
Atlassian	Bamboo Server & Data Center	All	Not Affected		Multiple Products Security Advisory - Log4j Vulnerable To Remote Code Execution - CVE-2021-44228	This product may be affected by a related but lower severity vulnerability if running in a specific non-default configuration.		
Atlassian	Bitbucket Server & Data Center	All	Affected	Yes	Multiple Products Security Advisory - Log4j Vulnerable To Remote Code Execution - CVE-2021-44228	This product is not vulnerable to remote code execution but may leak information due to the bundled Elasticsearch component being vulnerable.		
Atlassian	Confluence Server & Data Center	All	Not Affected		Multiple Products Security Advisory - Log4j Vulnerable To Remote Code Execution - CVE-2021-44228	This product may be affected by a related but lower severity vulnerability if running in a specific non-default configuration.		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Atlassian	Crowd Server & Data Center	All	Not Affected		Multiple Products Security Advisory - Log4j Vulnerable To Remote Code Execution - CVE-2021-44228	This product may be affected by a related but lower severity vulnerability if running in a specific non-default configuration.		
Atlassian	Crucible	All	Not Affected		Multiple Products Security Advisory - Log4j Vulnerable To Remote Code Execution - CVE-2021-44228	This product may be affected by a related but lower severity vulnerability if running in a specific non-default configuration.		
Atlassian	Fisheye	All	Not Affected		Multiple Products Security Advisory - Log4j Vulnerable To Remote Code Execution - CVE-2021-44228	This product may be affected by a related but lower severity vulnerability if running in a specific non-default configuration.		
Atlassian	Jira Server & Data Center	All	Not Affected		Multiple Products Security Advisory - Log4j Vulnerable To Remote Code Execution - CVE-2021-44228	This product may be affected by a related but lower severity vulnerability if running in a specific non-default configuration.		
Attivo networks					Attivo Networks Advisory			
AudioCodes					AudioCodes Link			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Autodesk			Under Investigation		Autodesk Article Link	Autodesk is continuing to perform a thorough investigation in relation to the recently discovered Apache Log4j security vulnerabilities. We continue to implement several mitigating factors for our products including patching, network firewall blocks, and updated detection signatures to reduce the threat of this vulnerability and enhance our ability to quickly respond to potential malicious activity. We have not identified any compromised systems in the Autodesk environment due to this vulnerability, at this time. This is an ongoing investigation and we will provide updates on the Autodesk Trust Center as we learn more.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Automox					Automox Blog Post			
Autopsy					Autopsy Link			
Auvik					Auvik Status Link			
Avantra SYSLINK					Avantra SYSLINK Article			
Avaya	Avaya Analytics	3.5, 3.6, 3.6.1, 3.7, 4	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Avaya Aura for OneCloud Private		Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security	Avaya is scanning and monitoring its OneCloud Private environments as part of its management activities. Avaya will continue to monitor this fluid situation and remediations will be made as patches become available, in accordance with appropriate change processes.		12/14/2021
Avaya	Avaya Aura® Application Enablement Services	8.1.3.2, 8.1.3.3, 10.1	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security		PSN020551u	12/14/2021
Avaya	Avaya Aura® Contact Center	7.0.2, 7.0.3, 7.1, 7.1.1, 7.1.2	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Avaya Aura® Device Services	8, 8.1, 8.1.4, 8.1.5	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Avaya Aura® Media Server	8.0.0, 8.0.1, 8.0.2	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security		PSN020549u	12/14/2021
Avaya	Avaya Aura® Presence Services	10.1, 7.1.2, 8, 8.0.1, 8.0.2, 8.1, 8.1.1, 8.1.2, 8.1.3, 8.1.4	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Avaya Aura® Session Manager	10.1, 7.1.3, 8, 8.0.1, 8.1, 8.1.1, 8.1.2, 8.1.3	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security		PSN020550u	12/14/2021
Avaya	Avaya Aura® System Manager	10.1, 8.1.3	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security		PSN005565u	12/14/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Avaya	Avaya Aura® Web Gateway	3.11[P], 3.8.1[P], 3.8[P], 3.9.1 [P], 3.9[P]	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Avaya Breeze™	3.7, 3.8, 3.8.1	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Avaya Contact Center Select	7.0.2, 7.0.3, 7.1, 7.1.1, 7.1.2	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Avaya CRM Connector - Connected Desktop	2.2	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Avaya Device Enablement Service	3.1.22	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Avaya Meetings	9.1.10, 9.1.11, 9.1.12	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Avaya one cloud private -UCaaS - Mid Market Aura	1	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Avaya OneCloud-Private	2	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Avaya Session Border Controller for Enterprise	8.0.1, 8.1, 8.1.1, 8.1.2, 8.1.3	Affected	Yes	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security		PSN020554u	12/14/2021
Avaya	Avaya Social Media Hub		Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Avaya Workforce Engagement	5.3	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Business Rules Engine	3.4, 3.5, 3.6, 3.7	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Callback Assist	5, 5.0.1	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Control Manager	9.0.2, 9.0.2.1	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Device Enrollment Service	3.1	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Equinox™ Conferencing	9.1.2	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Interaction Center	7.3.9	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Avaya	IP Office™ Platform	11.0.4, 11.1, 11.1.1, 11.1.2	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Proactive Outreach Manager	3.1.2, 3.1.3, 4, 4.0.1	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Avaya Aura® Device Services	8.0.1, 8.0.2, 8.1.3	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
AVEPOINT					AVEPOINT Notification			
AVM					AVM Link			
AvTech RoomAlert					AvTech RoomAlert Article			
AWS New					AWS New Security Bulletin			
AXON					AXON Link			
AXS Guard					AXS Guard Blog Post			
Axways Applications					Axways Applications Link			
B&R Industrial Automation	APROL		Not Affected		B&R Statement			12/16/2021
Baxter				Under Investigation	Baxter Advisory Link			12/20/2021
BackBox					BackBox Update			
Balbix					Balbix Blog Post			
Baramundi Products					Baramundi Products Forum			
Barco					Barco Link			
Barracuda					Barracuda Link			
BBraun	Outlook® Safety Infusion System Pump family		Not Affected	No	BBraun Advisory Link			12/20/2021
BBraun	Space® Infusion Pump family (Infusomat® Space® Infusion Pump, Perfusor® Space® Infusion		Not Affected	No	BBraun Advisory Link			12/20/2021
BBraun	Pump, SpaceStation, and Space® Wireless Battery)		Not Affected	No	BBraun Advisory Link			12/20/2021
BBraun	DoseTrac® Server, DoseLink™ Server, and Space® Online Suite Server software		Not Affected	No	BBraun Advisory Link			12/20/2021
BBraun	Pinnacle® Compounder		Not Affected	No	BBraun Advisory Link			12/20/2021
BBraun	APEX® Compounder		Not Affected	No	BBraun Advisory Link			12/20/2021
BD	Arctic Sun™ Analytics		Not Affected	No	BD Advisory Link			12/20/2021
BD	BD Diabetes Care App Cloud		Not Affected	No	BD Advisory Link			12/20/2021
BD	BD HealthSight™ Clinical Advisor		Not Affected	No	BD Advisory Link			12/20/2021
BD	BD HealthSight™ Data Manager		Not Affected	No	BD Advisory Link			12/20/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
BD	BD HealthSight™ Diversion Management		Not Affected	No	BD Advisory Link			12/20/2021
BD	BD HealthSight™ Infection Advisor		Not Affected	No	BD Advisory Link			12/20/2021
BD	BD HealthSight™ Inventory Optimization Analytics		Not Affected	No	BD Advisory Link			12/20/2021
BD	BD HealthSight™ Medication Safety		Not Affected	No	BD Advisory Link			12/20/2021
BD	BD Knowledge Portal for Infusion Technologies		Not Affected	No	BD Advisory Link			12/20/2021
BD	BD Knowledge Portal for Medication Technologies		Not Affected	No	BD Advisory Link			12/20/2021
BD	BD Knowledge Portal for BD Pyxis™ Supply		Not Affected	No	BD Advisory Link			12/20/2021
BD	BD Synapsys™ Informatics Solution		Not Affected	No	BD Advisory Link			12/20/2021
BD	BD Veritor™ COVID At Home Solution Cloud		Not Affected	No	BD Advisory Link			12/20/2021
Beckman Coulter			Under Investigation		Beckman Coulter Advisory Link			12/20/2021
Beijer Electronics	acirro+		Not Affected		Beijer Electronics Advisory Link			12/22/2021
Beijer Electronics	BFI frequency inverters		Not Affected		Beijer Electronics Advisory Link			12/22/2021
Beijer Electronics	BSD servo drives		Not Affected		Beijer Electronics Advisory Link			12/22/2021
Beijer Electronics	CloudVPN		Not Affected		Beijer Electronics Advisory Link			12/22/2021
Beijer Electronics	FnIO-G and M Distributed IO		Not Affected		Beijer Electronics Advisory Link			12/22/2021
Beijer Electronics	iX Developer		Not Affected		Beijer Electronics Advisory Link			12/22/2021
Beijer Electronics	Nexto modular PLC		Not Affected		Beijer Electronics Advisory Link			12/22/2021
Beijer Electronics	Nexto Xpress compact controller		Not Affected		Beijer Electronics Advisory Link			12/22/2021
Beijer Electronics	WARP Engineering Studio		Not Affected		Beijer Electronics Advisory Link			12/22/2021
BioMerieux			Under Investigation		BioMerieux Advisory Link			12/22/2021
Bender					Bender Link			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Best Practical Request Tracker (RT) and Request Tracker for Incident Response (RTIR)					Vendor Link			
BeyondTrust	Privilege Management Cloud	Unknown	Fixed	Yes	Security Advisory – Apache Log4j2 CVE 2021-44228 (Log4Shell)			2021-12-17
BeyondTrust	Privilege Management Reporting in BeyondInsight	21.2	Fixed	Yes	Security Advisory – Apache Log4j2 CVE 2021-44228 (Log4Shell)			2021-12-17
BeyondTrust	Secure Remote Access appliances	Unknown	Not Affected		Security Advisory – Apache Log4j2 CVE 2021-44228 (Log4Shell)			2021-12-17
BeyondTrust Bomgar					BeyondTrust Bomgar Link			
BisectHosting					BisectHosting Link			
BitDefender					BitDefender Advisory Link			
BitNami By VMware					BitNami By VMware			
BitRise					BitRise Post			
Bitwarden			Not Affected		Bitwarden Community Link			
Biztory	Fivetran		Not Affected		Apache Log4j2 Vulnerability - Updates For Biztory Clients		Vendor review indicated Fivetran is not vulnerable to Log4j2	
Black Kite					Black Kite Link			
Blancco					Blancco Support Link			
Blumira					Blumira Link			
BMC	Bladelogic Database Automation		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	BMC AMI Ops		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	BMC AMI Products		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	BMC Compuware		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	BMC Helix Automation Console		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	BMC Helix Business Workflows		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
BMC	BMC Helix Client Management		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	BMC Helix Cloud Cost		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	BMC Helix Cloud Security		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	BMC Helix CMDB		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	BMC Helix Continuous Optimization		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	BMC Helix Control-M		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	BMC Helix Digital Workplace		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	BMC Helix Discovery		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	BMC Helix ITSM		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	BMC Helix Knowledge Management		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	BMC Helix Operations Management with AIOps		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	BMC Helix Platform		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	BMC Helix platform		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
BMC	BMC Helix Remediate		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	BMC Helix Remediate		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	BMC Helix Remedyforce		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	BMC Helix Virtual Agent		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	Cloud Lifecycle Management		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	Control-M		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	Footprints		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	MainView Middleware Administrator		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	MainView Middleware Monitor		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	Remedy ITSM (IT Service Management)		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	SmartIT		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	Track-It!		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	TrueSight Automation for Networks		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
BMC	TrueSight Automation for Servers		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	TrueSight Capacity Optimization		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	TrueSight Infrastructure Management		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	TrueSight Operations Management		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
BMC	TrueSight Orchestration		Under Investigation		BMC Security Advisory for CVE-2021-44228 Log4Shell Vulnerability - Blogs & Documents - BMC Community			
Boston Scientific			Under Investigation		Boston Scientific Advisory Link			12/20/2021
Bosch			Affected	No	Bosch Advisory Link			12/22/2021
Box					Box Blog Post			
Brainworks					Brainworks Link			
BrightSign					BrightSign Link			
Broadcom	Advanced Secure Gateway (ASG)		Under Investigation		Broadcom Support Portal			
Broadcom	Automic Automation				Broadcome Automic Automation Link			
Broadcom	BCAAA		Under Investigation		Broadcom Support Portal			
Broadcom	CA Advanced Authentication	9.1	Affected					
Broadcom	CA Risk Authentication		Affected					
Broadcom	CA Strong Authentication		Affected					
Broadcom	Cloud Workload Protection (CWP)		Under Investigation		Broadcom Support Portal			
Broadcom	Cloud Workload Protection for Storage (CWP:S)		Under Investigation		Broadcom Support Portal			
Broadcom	CloudSOC Cloud Access Security Broker (CASB)		Not Affected		Broadcom Support Portal			
Broadcom	Content Analysis (CA)		Under Investigation		Broadcom Support Portal			
Broadcom	Critical System Protection (CSP)		Under Investigation		Broadcom Support Portal			
Broadcom	Data Center Security (DCS)		Not Affected		Broadcom Support Portal			
Broadcom	Data Loss Prevention (DLP)		Not Affected		Broadcom Support Portal			
Broadcom	Email Security Service (ESS)		Under Investigation		Broadcom Support Portal			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Broadcom	Ghost Solution Suite (GSS)		Not Affected		Broadcom Support Portal			
Broadcom	HSM Agent		Under Investigation		Broadcom Support Portal			
Broadcom	Industrial Control System Protection (ICSP)		Under Investigation		Broadcom Support Portal			
Broadcom	Integrated Cyber Defense Manager (ICDm)		Under Investigation		Broadcom Support Portal			
Broadcom	Integrated Secure Gateway (ISG)		Under Investigation		Broadcom Support Portal			
Broadcom	IT Management Suite		Not Affected		Broadcom Support Portal			
Broadcom	Layer7 API Developer Portal		Under Investigation		Broadcom Support Portal			
Broadcom	Layer7 API Gateway		Not Affected		Broadcom Support Portal			
Broadcom	Layer7 Mobile API Gateway		Not Affected		Broadcom Support Portal			
Broadcom	Management Center (MC)		Under Investigation		Broadcom Support Portal			
Broadcom	PacketShaper (PS) S-Series		Under Investigation		Broadcom Support Portal			
Broadcom	PolicyCenter (PC) S-Series		Under Investigation		Broadcom Support Portal			
Broadcom	Privileged Access Manager		Under Investigation		Broadcom Support Portal			
Broadcom	Privileged Access Manager Server Control		Under Investigation		Broadcom Support Portal			
Broadcom	Privileged Identity Manager		Under Investigation		Broadcom Support Portal			
Broadcom	ProxySG		Not Affected		Broadcom Support Portal			
Broadcom	Reporter		Under Investigation		Broadcom Support Portal			
Broadcom	Secure Access Cloud (SAC)		Under Investigation		Broadcom Support Portal			
Broadcom	Security Analytics (SA)		Not Affected		Broadcom Support Portal			
Broadcom	SiteMinder (CA Single Sign-On)		Under Investigation		Broadcom Support Portal			
Broadcom	SSL Visibility (SSLV)		Under Investigation		Broadcom Support Portal			
Broadcom	Symantec Control Compliance Suite (CCS)		Not Affected		Broadcom Support Portal			
Broadcom	Symantec Directory		Not Affected		Broadcom Support Portal			
Broadcom	Symantec Endpoint Detection and Response (EDR)		Under Investigation		Broadcom Support Portal			
Broadcom	Symantec Endpoint Encryption (SEE)		Under Investigation		Broadcom Support Portal			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Broadcom	Symantec Endpoint Protection (SEP)		Under Investigation		Broadcom Support Portal			
Broadcom	Symantec Endpoint Protection (SEP) for Mobile		Under Investigation		Broadcom Support Portal			
Broadcom	Symantec Endpoint Protection Manager (SEPM)	14.3	Affected	No	Broadcom Support Portal			
Broadcom	Symantec Identity Governance and Administration (IGA)		Not Affected		Broadcom Support Portal			
Broadcom	Symantec Mail Security for Microsoft Exchange (SMSMSE)		Under Investigation		Broadcom Support Portal			
Broadcom	Symantec Messaging Gateway (SMG)		Under Investigation		Broadcom Support Portal			
Broadcom	Symantec PGP Solutions		Not Affected		Broadcom Support Portal			
Broadcom	Symantec Protection Engine (SPE)		Under Investigation		Broadcom Support Portal			
Broadcom	Symantec Protection for SharePoint Servers (SPSS)		Under Investigation		Broadcom Support Portal			
Broadcom	VIP		Not Affected		Broadcom Support Portal			
Broadcom	VIP Authentication Hub		Under Investigation		Broadcom Support Portal			
Broadcom	Web Isolation (WI)		Under Investigation		Broadcom Support Portal			
Broadcom	Web Security Service (WSS)		Under Investigation		Broadcom Support Portal			
Broadcom	WebPulse		Under Investigation		Broadcom Support Portal			
C4b XPHONE					C4b XPHONE Link			
Camunda					Camunda Forum Link			
Canary Labs	All		Not Affected		Canary Labs Advisory Link			12/22/2021
Canon	CT Medical Imaging Products		Not Affected		Canon Advisory Link			12/22/2021
Canon	MR Medical Imaging Products		Not Affected		Canon Advisory Link			12/22/2021
Canon	UL Medical Imaging Products		Not Affected		Canon Advisory Link			12/22/2021
Canon	XR Medical Imaging Products		Not Affected		Canon Advisory Link			12/22/2021
Canon	NM Medical Imaging Products		Not Affected		Canon Advisory Link			12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Canon	Vitrea Advanced 7.x		Under Investigation		Canon Advisory Link			12/22/2021
Canon	Infinix-i (Angio Workstation)		Under Investigation		Canon Advisory Link			12/22/2021
Canon	Alphenix (Angio Workstation)		Under Investigation		Canon Advisory Link			12/22/2021
CapStorm	Copystorm		Under Investigation					12/22/2021
CarbonBlack					CarbonBlack Advisory			
Carestream			Not Affected		Carestream Advisory Link			12/20/2021
CAS genesisWorld					CAS genesisWorld Link			
Cato Networks					Cato Networks Blog Post			
Cepheid	C360		Not Affected		Cepheid Advisory Link			12/20/2021
Cepheid	GeneXpert		Under Investigation		Cepheid Advisory Link			12/20/2021
Cerberus FTP					Cerberus Article			
Chaser Systems	discrimiNAT Firewall	All	Not Affected		Are Chaser's products affected			
Check Point	CloudGuard	All	Not Affected		sk176865			
Check Point	Harmony Endpoint & Harmony Mobile	All	Not Affected		sk176865			
Check Point	Infinity Portal		Not Affected		sk176865			
Check Point	Quantum Security Gateway	All	Not Affected		sk176865			
Check Point	Quantum Security Management	All	Not Affected		sk176865	Where used, uses the 1.8.0_u241 version of the JRE that protects against this attack by default.		
Check Point	SMB	All	Not Affected		sk176865			
Check Point	ThreatCloud		Not Affected		sk176865			
CheckMK					CheckMK Forum			
Ciphermail					Ciphermail Blog Post			
CIS					CIS Customer Portal			
Cisco	AppDynamics		Affected	Yes	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Common Services Platform Collector		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Network Services Orchestrator (NSO)		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco System Architecture Evolution Gateway (SAEGW)		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco ACI Multi-Site Orchestrator		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cisco	Cisco ACI Virtual Edge		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Adaptive Security Appliance (ASA) Software		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Advanced Web Security Reporting Application		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco AMP Virtual Private Cloud Appliance		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco AnyConnect Secure Mobility Client		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Application Policy Infrastructure Controller (APIC)		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco ASR 5000 Series Routers		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Broadcloud Calling		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco BroadWorks		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Catalyst 9800 Series Wireless Controllers		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco CloudCenter Suite Admin		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco CloudCenter Workload Manager		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Cognitive Intelligence		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Computer Telephony Integration Object Server (CTIOS)		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Connected Grid Device Manager		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Connected Mobile Experiences		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cisco	Cisco Connectivity		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Contact Center Domain Manager (CCDM)		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Contact Center Management Portal (CCMP)		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Crosswork Change Automation		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco CX Cloud Agent Software		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Data Center Network Manager (DCNM)		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Defense Orchestrator		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco DNA Assurance		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco DNA Center		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco DNA Spaces		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	DUO network gateway (on-prem/self-hosted)		Under Investigation					
Cisco	Cisco Elastic Services Controller (ESC)		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Emergency Responder		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Enterprise Chat and Email		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Enterprise NFV Infrastructure Software (NFVIS)		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Evolved Programmable Network Manager		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cisco	Cisco Extensible Network Controller (XNC)		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Finesse		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Firepower Management Center		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Firepower Threat Defense (FTD)		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco GGSN Gateway GPRS Support Node		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco HyperFlex System		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Identity Services Engine (ISE)		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Integrated Management Controller (IMC) Supervisor		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Intersight		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Intersight Virtual Appliance		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco IOS and IOS XE Software		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco IoT Field Network Director (formerly Cisco Connected Grid Network Management System)		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco IoT Operations Dashboard		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco IOx Fog Director		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco IP Services Gateway (IPSG)		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cisco	Cisco Kinetic for Cities		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco MDS 9000 Series Multilayer Switches		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Meeting Server		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco MME Mobility Management Entity		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Modeling Labs		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Network Assessment (CNA) Tool		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Network Assurance Engine		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Network Convergence System 2000 Series		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Network Planner		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Nexus 5500 Platform Switches		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Nexus 5600 Platform Switches		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Nexus 6000 Series Switches		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Nexus 7000 Series Switches		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Nexus Dashboard (formerly Cisco Application Services Engine)		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Nexus Data Broker		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cisco	Cisco Nexus Insights		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Optical Network Planner		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Packaged Contact Center Enterprise		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Paging Server (InformaCast)		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Paging Server		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco PDSN/HA Packet Data Serving Node and Home Agent		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cis co Products: December 2021			
Cisco	Cisco PGW Packet Data Network Gateway		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Policy Suite		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Prime Central for Service Providers		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Prime Collaboration Manager		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Prime Collaboration Provisioning		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Prime Infrastructure		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Prime License Manager		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Prime Network		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Prime Optical for Service Providers		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Prime Provisioning		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cisco	Cisco Prime Service Catalog		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Registered Envelope Service		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco SD-WAN vEdge 1000 Series Routers		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco SD-WAN vEdge 2000 Series Routers		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco SD-WAN vEdge 5000 Series Routers		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco SD-WAN vEdge Cloud Router Platform		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco SD-WAN vManage		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Secure Network Analytics (SNA), formerly Stealthwatch		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco SocialMiner		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco TelePresence Management Suite		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco UCS Director		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco UCS Performance Manager		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Umbrella		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Unified Attendant Console Advanced		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Unified Attendant Console Business Edition		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Unified Attendant Console Department Edition		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cisco	Cisco Unified Attendant Console Enterprise Edition		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Unified Attendant Console Premium Edition		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Unified Communications Manager Cloud		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Unified Contact Center Enterprise - Live Data server		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Unified Contact Center Enterprise		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Unified Contact Center Express		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Unified Intelligent Contact Management Enterprise		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Unified SIP Proxy Software		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Video Surveillance Operations Manager		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Virtual Topology System - Virtual Topology Controller (VTC) VM		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Virtualized Voice Browser		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Vision Dynamic Signage Director		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco WAN Automation Engine (WAE)		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Web Security Appliance (WSA)		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Webex Cloud-Connected UC (CCUC)		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cisco	Cisco Webex Meetings Server		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Webex Teams		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Wide Area Application Services (WAAS)		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Duo		Not Affected	Yes	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	duo network gateway (on-prem/self-hosted)		Under Investigation					
Cisco	Exony Virtualized Interaction Manager (VIM)		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Managed Services Accelerator (MSX) Network Access Control Service		Under Investigation		Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Citrix	Citrix ADC (NetScaler ADC) and Citrix Gateway (NetScaler Gateway)	All Platforms	Not Affected		Citrix Statement	Citrix continues to investigate any potential impact on Citrix-managed cloud services. If, as the investigation continues, any Citrix-managed services are found to be affected by this issue, Citrix will take immediate action to remediate the problem. Customers using Citrix-managed cloud services do not need to take any action.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Citrix	Citrix Application Delivery Management (NetScaler MAS)	All Platforms	Not Affected		Citrix Statement	Citrix continues to investigate any potential impact on Citrix-managed cloud services. If, as the investigation continues, any Citrix-managed services are found to be affected by this issue, Citrix will take immediate action to remediate the problem. Customers using Citrix-managed cloud services do not need to take any action.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Citrix	Citrix Cloud Connector		Not Affected		Citrix Statement	Citrix continues to investigate any potential impact on Citrix-managed cloud services. If, as the investigation continues, any Citrix-managed services are found to be affected by this issue, Citrix will take immediate action to remediate the problem. Customers using Citrix-managed cloud services do not need to take any action.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Citrix	Citrix Connector Appliance for Cloud Services		Not Affected		Citrix Statement	Citrix continues to investigate any potential impact on Citrix-managed cloud services. If, as the investigation continues, any Citrix-managed services are found to be affected by this issue, Citrix will take immediate action to remediate the problem. Customers using Citrix-managed cloud services do not need to take any action.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Citrix	Citrix Content Collaboration (ShareFile Integration) – Citrix Files for Windows, Citrix Files for Mac, Citrix Files for Outlook		Not Affected		Citrix Statement	Citrix continues to investigate any potential impact on Citrix-managed cloud services. If, as the investigation continues, any Citrix-managed services are found to be affected by this issue, Citrix will take immediate action to remediate the problem. Customers using Citrix-managed cloud services do not need to take any action.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Citrix	Citrix Endpoint Management (Citrix XenMobile Server)		Affected	Yes	Citrix Statement	For CVE-2021-44228 and CVE-2021-45046: Impacted–Customers are advised to apply the latest CEM rolling patch updates listed below as soon as possible to reduce the risk of exploitation. XenMobile Server 10.14 RP2; XenMobile Server 10.13 RP5; and XenMobile Server 10.12 RP10. Note: Customers who have upgraded their XenMobile Server to the updated versions are recommended not to apply the responder policy mentioned in the blog listed below to the Citrix ADC vserver in front of the XenMobile Server as it may impact the enrollment of Android devices. For CVE-2021-45105: Investigation in progress.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Citrix	Citrix Hypervisor (XenServer)		Not Affected		Citrix Statement	Citrix continues to investigate any potential impact on Citrix-managed cloud services. If, as the investigation continues, any Citrix-managed services are found to be affected by this issue, Citrix will take immediate action to remediate the problem. Customers using Citrix-managed cloud services do not need to take any action.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Citrix	Citrix License Server		Not Affected		Citrix Statement	Citrix continues to investigate any potential impact on Citrix-managed cloud services. If, as the investigation continues, any Citrix-managed services are found to be affected by this issue, Citrix will take immediate action to remediate the problem. Customers using Citrix-managed cloud services do not need to take any action.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Citrix	Citrix SD-WAN	All Platforms	Not Affected		Citrix Statement	Citrix continues to investigate any potential impact on Citrix-managed cloud services. If, as the investigation continues, any Citrix-managed services are found to be affected by this issue, Citrix will take immediate action to remediate the problem. Customers using Citrix-managed cloud services do not need to take any action.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Citrix	ShareFile Storage Zones Controller		Not Affected		Citrix Statement	Citrix continues to investigate any potential impact on Citrix-managed cloud services. If, as the investigation continues, any Citrix-managed services are found to be affected by this issue, Citrix will take immediate action to remediate the problem. Customers using Citrix-managed cloud services do not need to take any action.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Citrix	Citrix Virtual Apps and Desktops (XenApp & XenDesktop)		Affected		Citrix Statement	IMPACTED: Linux VDA (non-LTSR versions only)- CVE-2021-44228 and CVE-2021-45046: Customers are advised to apply the latest update as soon as possible to reduce the risk of exploitation. Linux Virtual Delivery Agent 2112. See the Citrix Statement for additional mitigations. For CVE-2021-45105: Investigation has shown that Linux VDA is not impacted. Nonetheless, the Linux VDA 2112 has been updated (21.12.0.30, released December 20th) to contain Apache log4j version 2.17.0. NOT IMPACTED: Linux VDA LTSR all versions; All other CVAD components.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Citrix	Citrix Workspace App	All Platforms	Not Affected		Citrix Statement	Citrix continues to investigate any potential impact on Citrix-managed cloud services. If, as the investigation continues, any Citrix-managed services are found to be affected by this issue, Citrix will take immediate action to remediate the problem. Customers using Citrix-managed cloud services do not need to take any action.		12/21/2021
Claris					Claris Article			
Cloudera	AM2CM Tool		Not Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Ambari	Only versions 2.x, 1.x	Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Arcadia Enterprise	Only version 7.1.x	Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	CDH, HDP, and HDF	Only version 6.x	Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cloudera	CDP Operational Database (COD)		Not Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	CDP Private Cloud Base	Only version 7.x	Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	CDS 3 Powered by Apache Spark	All versions	Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	CDS 3.2 for GPUs	All versions	Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Cloudera Cybersecurity Platform	All versions	Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Cloudera Data Engineering (CDE)		Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Cloudera Data Engineering (CDE)	All versions	Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Cloudera Data Flow (CFM)		Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Cloudera Data Science Workbench (CDSW)	Only versions 2.x, 3.x	Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Cloudera Data Visualization (CDV)		Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Cloudera Data Warehouse (CDW)		Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cloudera	Cloudera Data Warehouse (CDW)	All versions	Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Cloudera DataFlow (CDF)		Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Cloudera Edge Management (CEM)	All versions	Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Cloudera Enterprise	Only version 6.x	Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Cloudera Flow Management (CFM)	All versions	Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Cloudera Machine Learning (CML)		Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Cloudera Machine Learning (CML)	All versions	Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Cloudera Manager (Including Backup Disaster Recovery (BDR) and Replication Manager)	All versions	Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Cloudera Manager (Including Backup Disaster Recovery (BDR) and Replication Manager)	Only versions 7.0.x, 7.1.x, 7.2.x	Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Cloudera Manager (Including Backup Disaster Recovery (BDR))		Not Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cloudera	Cloudera Runtime (including Cloudera Data Hub and all Data Hub templates)	Only versions 7.0.x, 7.1.x, 7.2.x	Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Cloudera Stream Processing (CSP)	All versions	Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Cloudera Streaming Analytics (CSA)		Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Cloudera Streaming Analytics (CSA)		Not Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Data Analytics Studio (DAS)		Under Investigation		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Data Catalog		Not Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Data Lifecycle Manager (DLM)		Not Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Data Steward Studio (DSS)	All versions	Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Hortonworks Data Flow (HDF)		Not Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Hortonworks Data Platform (HDP)	Only versions 7.1.x, 2.7.x, 2.6.x	Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Hortonworks DataPlane Platform		Not Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cloudera	Management Console	All versions	Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Management Console for CDP Public Cloud		Not Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Replication Manager		Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	SmartSense		Under Investigation		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Workload Manager		Not Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Workload XM (SaaS)		Not Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
Cloudera	Workload XM	All versions	Affected		https://my.cloudera.com/knowledge/TSB-2021-545-Critical-vulnerability-in-log4j2-CVE-2021-44228?id=332019			
CloudFlare					CloudFlare Blog Post			
Cloudian HyperStore					Cloudian Article			
Cloudogu	Ecosystem	All	Affected	Yes	Cloudogu Community			
Cloudogu	SCM-Manager		Not Affected		SCM-Manager Blog			
Cloudron					Cloudron Forum			
Clover					Clover Article			
Code42	Code42 App	8.8.1	Fixed	Yes	Code42 Release Notification			12/22/2021
Code42	Crashplan	8.8, possibly prior versions	Fixed	Yes	Code42 Release Notification	I think, they don't specify in the notice, but we know that they released an updated Crashplan client. Possibly prior versions affected.		12/16/2021
CodeBeamer					CodeBeamer Link			
Codesys					Codesys News			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cohesity					Cohesity Support Link			
CommVault					CommVault Documentation			
Concourse	Concourse		Not affected		Concourse Community Discussion			
ConcreteCMS.com					ConcreteCMS.com Link			
Confluent	Confluent Cloud	N/A	Fixed		December 2021 Log4j Vulnerabilities Advisory			12/17/2021
Confluent	Confluent Platform	<7.0.1	Affected	Yes	December 2021 Log4j Vulnerabilities Advisory			12/17/2021
Confluent	Confluent for Kubernetes	N/A	Not Affected		December 2021 Log4j Vulnerabilities Advisory			12/17/2021
Confluent	Confluent Kafka Connectors	N/A	Not Affected	N/A	December 2021 Log4j Vulnerabilities Advisory			12/17/2021
Confluent	Confluent ElasticSearch Sink Connector	<11.1.7	Affected	Yes	December 2021 Log4j Vulnerabilities Advisory			12/17/2021
Confluent	Confluent Google DataProc Sink Connector	<1.1.5	Affected	Yes	December 2021 Log4j Vulnerabilities Advisory			12/17/2021
Confluent	Confluent Splunk Sink Connector	<2.05	Affected	Yes	December 2021 Log4j Vulnerabilities Advisory			12/17/2021
Confluent	Confluent HDFS 2 Sink Connector	<10.1.3	Affected	Yes	December 2021 Log4j Vulnerabilities Advisory			12/17/2021
Confluent	Confluent HDFS 3 Sink Connector	<1.1.8	Affected		December 2021 Log4j Vulnerabilities Advisory			12/17/2021
Confluent	Confluent VMWare Tanzu GemFire Sink Connector	<1.0.8	Affected	Yes	December 2021 Log4j Vulnerabilities Advisory			12/17/2021
Connect2id					Connect2id Blog Post			
ConnectWise					ConnectWise Advisory Link			
ContrastSecurity					ContrastSecurity Article			
ControlUp					ControlUp Link			
COPADATA					COPADATA Support Services			
CouchBase					CouchBase Forums			
CPanel					CPanel Forms			
Cradlepoint					Cradlepoint			
Crestron			Not Affected		Crestron Advisory			12/20/2021
CrushFTP					CrushFTP Link			
CryptShare					Cryptshare Support Link			
CyberArk	Privileged Threat Analytics (PTA)	N/A	Fixed	Yes	CyberArk Customer Force		This advisory is available to customers only and has not been reviewed by CISA.	12/14/2021
Cybereason					Cybereason Blog Post			
CyberRes					CyberRes Community Link			
DarkTrace					DarkTrace Customer Portal			
Dassault Systèmes					Dassault Systemes Link			
Databricks					Databricks Google Doc			
Datadog	Datadog Agent	>=6.17.0, <=6.32.2, >=7.17.0, <=7.32.2	Fixed	Yes	Datadog Log4j Vulnerability Update			
Dataminer					Dataminer Community Link			
Datev					Datev Community Link			
Datto					Datto Link			
dCache.org					dCache.org Link			
Debian					Debian Tracker Link			
Deepinstinct					Deepinstinct Link			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	Alienware Command Center	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Alienware OC Controls	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Alienware On Screen Display	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Alienware Update	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Atmos	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Azure Stack HCI	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	CalMAN Powered Calibration Firmware	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	CalMAN Ready for Dell	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Centera	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Chameleon Linux Based Diagnostics	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Chassis Management Controller (CMC)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	China HDD Deluxe	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Cloud Mobility for Dell EMC Storage	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Cloud Tiering Appliance	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Connectrix (Cisco MDS 9000 switches)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Connextrix B Series	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	CyberSecIQ Application	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	CyberSense for PowerProtect Cyber Recovery	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell BSAFE Crypto-C Micro Edition	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell BSAFE Crypto-J	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell BSAFE Micro Edition Suite	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Calibration Assistant	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Cinema Color	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Cloud Command Repository Manager	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Cloud Management Agent	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Color Management	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Command Configure	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Command Integration Suite for System Center	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Command Intel vPro Out of Band	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Command Monitor	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Command Power Manager	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Command PowerShell Provider	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Command Update	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Customer Connect	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	Dell Data Guardian*	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Data Protection*	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Data Recovery Environment	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Data Vault	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Data Vault for Chrome OS	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Deployment Agent	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Digital Delivery	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Direct USB Key	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Display Manager 1.5 for Windows / macOS	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Display Manager 2.0 for Windows / macOS	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC AppSync	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC Cloudboost	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC CloudLink	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC Container Storage Modules	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC Data Computing Appliance (DCA)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC Data Protection Advisor	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC DataIQ	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	Dell EMC Disk Library for Mainframe	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC GeoDrive	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC Isilon InsightIQ	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC License Manager	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC Networking Onie	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC OpenManage Ansible Modules	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC OpenManage integration for Splunk	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC OpenManage Integration for VMware vCenter	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC OpenManage Management pack for vRealize Operations	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC OpenManage Operations Connector for Micro Focus Operations Bridge Manager	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	"Dell EMC PowerMax VMAX VMAX3 and VMAX AFA"	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC PowerPath	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC PowerPath Management Appliance	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC PowerProtect Cyber Recovery	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC PowerScale OneFS	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	Dell EMC PowerShell for PowerMax	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC PowerShell for Powerstore	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC PowerShell for Unity	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	“Dell EMC PowerSwitch Z9264F-ON BMC Dell EMC PowerSwitch Z9432F-ON BMC”	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC PowerVault ME4 Series Storage Arrays	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC PowerVault MD3 Series Storage Arrays	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC Repository Manager (DRM)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC SourceOne	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC Systems Update (DSU)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC Unisphere 360	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC Virtual Storage Integrator	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC VPLEX	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell EMC XtremIO	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Encryption Enterprise*	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Encryption Personal*	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Endpoint Security Suite Enterprise*	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	Dell Hybrid Client	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell ImageAssist	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Insights Client	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Linux Assistant	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Mobile Connect	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Monitor ISP (Windows/Mac/Linux)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Monitor SDK	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Networking X-Series	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Open Manage Mobile	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Open Manage Server Administrator	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell OpenManage Change Management	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell OpenManage Enterprise Power Manager Plugin	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Optimizer	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell OS Recovery Tool	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Peripheral Manager 1.4 / 1.5 for Windows	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Platform Service	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	Dell Power Manager	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Power Manager Lite	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Precision Optimizer	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Precision Optimizer for Linux	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Premier Color	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Recovery (Linux)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Remediation Platform	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Remote Execution Engine (DRONE)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Security Advisory Update - DSA-2021-088	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Security Management Server & Dell Security Management Server Virtual*	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell SupportAssist SOS	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Thin OS	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Threat Defense	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell True Color	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Trusted Device	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Dell Update	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	Dream Catcher	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	DUP Creation Service	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	DUP Framework (ISG)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Embedded NAS	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Embedded Service Enabler	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Equallogic PS	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Fluid FS	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	iDRAC Service Module (iSM)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Infinity MLK (firmware)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Integrated Dell Remote Access Controller (iDRAC)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	ISG Accelerators	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	ISG Board & Electrical	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	IsilonSD Management Server	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	IVE-WinDiag	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Mainframe Enablers	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	My Dell	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	MyDell Mobile	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	NetWorker Management Console	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Networking BIOS	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Networking DIAG	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Networking N-Series	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Networking OS 10	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Networking OS9	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Networking SD-WAN Edge SD-WAN	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Networking W-Series	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Networking X-Series	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	OMIMSSC (OpenManage Integration for Microsoft System Center)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	OMNIA	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	OpenManage Connections - Nagios	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	OpenManage Connections - ServiceNow	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	OpenManage Integration for Microsoft System Center for System Center Operations Manager	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	OpenManage Integration with Microsoft Windows Admin Center	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	OpenManage Network Integration	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	PowerConnect N3200	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	PowerConnect PC2800	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	PowerConnect PC8100	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	PowerEdge BIOS	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	PowerEdge Operating Systems	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	PowerTools Agent	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	PPDM Kubernetes cProxy	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	PPDM VMware vProxy	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Redtail	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Remotely Anywhere	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Riptide (firmware)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Rugged Control Center (RCC)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	SD ROM Utility	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	SDNAS	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Server Storage	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Smart Fabric Storage Software	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	SmartByte	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	SMI-S	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Software RAID	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Solutions Enabler	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Solutions Enabler vApp	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Sonic	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	SRS VE	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Storage Center OS and additional SC applications unless otherwise noted	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	SupportAssist Client Commercial	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	SupportAssist Client Consumer	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	UCC Edge	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Unisphere for PowerMax	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Unisphere for PowerMax vApp	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Unisphere for VMAX	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Unisphere for VNX	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Update Manager Plugin	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	ViPR Controller	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	VNX1	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	VNX2	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	VPLEX VS2/VS6 / VPLEX Witness	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Vsan Ready Nodes	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Warnado MLK (firmware)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Wyse Proprietary OS (ThinOS)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	Wyse Windows Embedded Suite	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			12/15/2021
Dell	APEX Console	N/A	Fixed	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Cloud environment patched		12/15/2021
Dell	APEX Data Storage Services		Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Cloud environment patch in progress		12/15/2021
Dell	Cloud IQ		Fixed	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Cloud environment patched		12/15/2021
Dell	Connectrix (Cisco MDS DCNM)		Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch expected by 12/23/21		12/15/2021
Dell	Connectrix B-Series SANnav	2.1.1	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch expected by 3/31/2022		12/15/2021
Dell	Data Domain OS	Versions between 7.3.0.5 and 7.7.0.6;Versions before 7.6.0.30	Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	See DSA-2021-274		12/15/2021
Dell	Dell EMC Avamar	"18.2 19.1 19.2 19.3 19.4"	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch expected by 12/20/21		12/15/2021
Dell	Dell EMC BSN Controller Node		Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	See DSA-2021-305		12/15/2021
Dell	Dell EMC Cloud Disaster Recovery	N/A	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch pending		12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	Dell EMC Data Protection Central		Affected		Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	See DSA-2021-269		12/15/2021
Dell	Dell EMC Data Protection Search	Versions before 19.5.0.7	Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	See DSA-2021-279		12/15/2021
Dell	Dell EMC ECS		Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch expected by 12/18/21		12/15/2021
Dell	Enterprise Hybrid Cloud		Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	link		12/15/2021
Dell	Dell EMC Enterprise Storage Analytics for vRealize Operations	"<6.0.0 6.1.0 6.2.x"	Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	See DSA-2021-278		12/15/2021
Dell	Dell EMC Integrated System for Azure Stack HCI	N/A	Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	"Dell EMC Integrated System for Azure Stack HCI is not impacted by this advisory. If Dell EMC SupportAssist Enterprise (SAE) or Dell EMC Secure Connect Gateway (SCG) were optionally installed with Dell EMC Integrated System for Azure Stack HCI monitor the following advisories. Apply workaround guidance and remediations as they become available:		12/15/2021
Dell	Dell EMC Integrated System for Microsoft Azure Stack Hub	N/A	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch pending		12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	Dell EMC NetWorker Virtual Edition	“19.5.x 19.4.x 19.3.x”	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch expected by 12/20/21		12/15/2021
Dell	Dell EMC NetWorker Server	“19.5.x 19.4.x 19.3.x”	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch expected by 12/20/21		12/15/2021
Dell	Dell EMC Networking Virtual Edge Platform with VersaOS	“with Versa Concerto with Versa Analytics with Versa Concero Director”	Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	See DSA-2021-304		12/15/2021
Dell	Dell EMC PowerFlex Appliance	“All versions up to Intelligent Catalog 38_356_00_r10.zip All versions up to Intelligent Catalog 38_362_00_r7.zip”	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch pending		12/15/2021
Dell	Dell EMC PowerFlex Software (SDS)	“3.5 3.5.1 3.5.1.1 3.5.1.2 3.5.1.3 3.5.1.4 3.6 3.6.0.1 3.6.0.2”	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch pending		12/15/2021
Dell	Dell EMC PowerFlex Rack	N/A	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch pending		12/15/2021
Dell	Dell EMC PowerProtect Data Manager	All versions 19.9 and earlier	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch pending		12/15/2021
Dell	Dell EMC PowerProtect DP Series Appliance (iDPA)	2.7.0 and earlier	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch pending		12/15/2021
Dell	Dell EMC PowerStore		Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch expected by 12/23/21		12/15/2021
Dell	Dell EMC RecoverPoint for Virtual Machine	All 5.0.x and later versions	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch pending		12/15/2021
Dell	Dell EMC RecoverPoint Classic	All 5.1.x and later versions	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch pending		12/15/2021
Dell	Dell EMC SRM vApp	Versions before 4.6.0.2	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch expected by 1/25/2022		12/15/2021
Dell	Dell EMC Streaming Data Platform		Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch expected by 12/18/21		12/15/2021
Dell	Dell EMC Unity		Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch expected by 12/29/21		12/15/2021
Dell	Dell EMC Metro Node	7.0.x	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	See DSA-2021-308		12/15/2021
Dell	Dell EMC VxRail	“4.5.x 4.7.x 7.0.x”	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch pending		12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	Dell Open Management Enterprise - Modular	<1.40.10	Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	See DSA-2021-268		12/15/2021
Dell	DellEMC OpenManage Enterprise Services		Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch expected by 12/20/21		12/15/2021
Dell	OpenManage Enterprise		Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch expected by 12/19/21		12/15/2021
Dell	Dell EMC Ruckus SmartZone 300 Controller		Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	See DSA-2021-303		12/15/2021
Dell	Dell EMC Ruckus SmartZone 100 Controller		Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	See DSA-2021-303		12/15/2021
Dell	Dell EMC Ruckus Virtual Software		Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	See DSA-2021-303		12/15/2021
Dell	Secure Connect Gateway (SCG) Appliance	“5.00.00 5.00.05 and 4.0.06 and earlier versions (OVF and VHD)”	Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	See DSA-2021-282		12/15/2021
Dell	Secure Connect Gateway (SCG) Policy Manager	“5.00.00.10 5.00.05.10”	Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	See DSA-2021-281		12/15/2021
Dell	SRS Policy Manager	7	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch pending		12/15/2021
Dell	Storage Center - Dell Storage Manager		Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch pending		12/15/2021
Dell	SupportAssist Enterprise		Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch expected by 12/23/21		12/15/2021
Dell	Unisphere Central		Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch expected by 1/10/2022		12/15/2021
Dell	Vblock		Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch pending See vce6771 (requires customer login)		12/15/2021
Dell	VNXe 1600	Versions 3.1.16.10220572 and earlier	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch expected by 12/19/21		12/15/2021
Dell	VNXe 3200	Version 3.1.15.10216415 and earlier	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch expected by 12/19/21		12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	VxBlock		Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	“Patch pending See vce6771 (requires customer login)”		12/15/2021
Dell	vRealize Orchestrator (vRO) Plug-ins for Dell EMC Storage	Various	Affected		Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	See DSA-2021-300		12/15/2021
Dell	vRO Plugin for Dell EMC PowerMax	Version 1.2.3 or earlier	Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	See DSA-2021-300		12/15/2021
Dell	vRO Plugin for Dell EMC PowerScale	Version 1.1.0 or earlier	Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	See DSA-2021-300		12/15/2021
Dell	vRO Plugin for Dell EMC PowerStore	Version 1.1.4 or earlier	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	See DSA-2021-300		12/15/2021
Dell	vRO Plugin for Dell EMC Unity	Version 1.0.6 or earlier	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	See DSA-2021-300		12/15/2021
Dell	vRO Plugin for Dell EMC XtremIO	Version 4.1.2 or earlier	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	See DSA-2021-300		12/15/2021
Dell	vRealize Data Protection Extension Data Management		Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch expected by 12/19/21		12/15/2021
Dell	vRealize Data Protection Extension for vRealize Automation (vRA) 8.x	“version 19.6 version 19.7 version 19.8 and version 19.9”	Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch expected by 12/19/21		12/15/2021
Dell	VMware vRealize Automation 8.x	“8.2 8.3 8.4 8.5 and 8.6”	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch expected by 12/19/21		12/15/2021
Dell	VMware vRealize Orchestrator 8.x	“8.2 8.3 8.4 8.5 and 8.6”	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch expected by 12/19/21		12/15/2021
Dell	Wyse Management Suite	<3.5	Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	See DSA-2021-267		12/15/2021
Deltares	Delft-FEWS	>2018.02	Fixed	No	Deltares Advisory	Mitigations Only		12/22/2021
Denequa					Denequa Link			
Device42					Device42 Link			
Devolutions	All products		Not Affected		https://blog.devolutions.net/2021/12/critical-vulnerability-in-log4j/			
Diebold Nixdorf					Diebold Nixdorf Link			
Digi International	CTEK G6200 family		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	CTEK SkyCloud		Not Affected		Digi International Advisory Link			12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Digi International	CTEK Z45 family		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi 54xx family		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi 63xx family		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi AnywhereUSB (G2) family		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi AnywhereUSB Plus family		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi Connect family		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi Connect EZ family		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi Connect IT family		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi ConnectPort family		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi ConnectPort LTS family		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi Connect Sensor family		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi Connect WS family		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi Embedded Android		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi Embedded Yocto		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi EX routers		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi IX routers		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi LR54		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi One family		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi Passport family		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi PortServer TS family		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi TX routers		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi WR11		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi WR21		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi WR31		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi WR44R/RR		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi WR54		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi WR64		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	AnywhereUSB Manager		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Aview		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	ARMT		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	AVWOB		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi Navigator		Not Affected		Digi International Advisory Link			12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Digi International	Digi Remote Manager		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi Xbee mobile app		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Lighthouse		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Realport		Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Remote Hub Config Utility		Not Affected		Digi International Advisory Link			12/21/2021
Digicert					Digicert Link			
Digital AI					Digital AI Article			
DNSFilter					DNSFilter Blog Post			
Docker					Docker Blog Post			
Docusign					Docusign Alert			
DrayTek	Vigor Routers, Access Points, Switches, VigorACS Central Management Software, MyVigor Platform		Not Affected		DrayTek Statement			12/15/2021
DSpace					DSpace Google Group			
Dynatrace	Managed cluster nodes		Not Affected	No	Official Dynatrace Communication	Please see Dynatrace Communication for details		12/21/2021
Dynatrace	SAAS		Fixed	No	Official Dynatrace Communication			12/21/2021
Dynatrace	FedRamp SAAS		Fixed	No	Official Dynatrace Communication			12/21/2021
Dynatrace	Synthetic public locations		Fixed	No	Official Dynatrace Communication			12/21/2021
Dynatrace	Synthetic Private ActiveGate		Fixed	Yes	Official Dynatrace Communication	Please see Dynatrace Communication for details		12/21/2021
Dynatrace	ActiveGate		Not Affected	No	Official Dynatrace Communication			12/21/2021
Dynatrace	OneAgent		Not Affected	No	Official Dynatrace Communication			12/21/2021
Dynatrace	Dynatrace Extensions		Fixed	Yes (See Notes)	Official Dynatrace Communication	Please see Dynatrace Communication for details		12/21/2021
EasyRedmine					EasyRedmine News			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Eaton	Undisclosed	Undisclosed	Affected		Security Bulletin	Doesn’t openly disclose what products are affected or not for quote ‘security purposes’. Needs email registration. No workaround provided due to registration wall.		
EclecticIQ					EclecticIQ Advisory			
Eclipse Foundation					Eclipse Foundation Wiki			
EFI					EFI Link			
EGroupware					EGroupware Link			
Elastic	APM Java Agent		Under Investigation		Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31			12/15/2021
Elastic	APM Server		Not Affected		Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31			12/15/2021
Elastic	Beats		Not Affected		Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31			12/15/2021
Elastic	Cmd		Not Affected		Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31			12/15/2021
Elastic	Elastic Agent		Not Affected		Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31			12/15/2021
Elastic	Elastic Cloud Enterprise		Under Investigation		Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31			12/15/2021
Elastic	Elastic Cloud Enterprise		Under Investigation		Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31			12/15/2021
Elastic	Elastic Cloud on Kubernetes		Not Affected		Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Elastic	Elastic Cloud		Under Investigation		Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31			12/15/2021
Elastic	Elastic Endgame		Not Affected		Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31			12/15/2021
Elastic	Elastic Maps Service		Not Affected		Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31			12/15/2021
Elastic	Elasticsearch	5,6,8	Affected	Yes	Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31			12/15/2021
Elastic	Endpoint Security		Not Affected		Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31			12/15/2021
Elastic	Enterprise Search		Not Affected		Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31			12/15/2021
Elastic	Fleet Server		Not Affected		Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31			12/15/2021
Elastic	Kibana		Not Affected		Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31			12/15/2021
Elastic	Logstash	<6.8.21,<7.16.1	Affected	Yes	Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31			12/15/2021
Elastic	Machine Learning		Not Affected		Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31			12/15/2021
Elastic	Swiftype		Not Affected		Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31			12/15/2021
ElasticSearch	all products		Not Affected					
Ellucian	Banner Analytics		Affected	No	Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Colleague		Affected	No	Ellucian Response on Apache Log4j Issue	On-prem and cloud deployements expect fixed 12/18/2021		12/17/2021
Ellucian	Admin		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Ellucian	Enterprise Identity Services(BEIS)		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Banner Integration for eLearning		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Banner Integration for eProcurement		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Banner Workflow		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Banner Document Management (includes Banner Document Retention)		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Ellucian Advance Web Connector		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Ellucian eTranscripts		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Ellucian Mobile		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Ellucian Solution Manager		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Banner Event Publisher		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Banner Self Service		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Colleague Analytics		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	CRM Advance		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	CRM Advise		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	CRM Recruit		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Ellucian Data Access		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Ellucian Design Path		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Ellucian ePrint		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Ellucian Ethos API & API Management Center		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Ellucian Ethos Extend		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Ellucian Ethos Integration		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Ellucian Experience		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Ellucian Intelligent Platform (ILP)		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Ellucian International Student and Scholar Management (ISSM)		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Ellucian Message Service (EMS)		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Ellucian	Ellucian Messaging Adapter (EMA)		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Ellucian Payment Gateway		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Ellucian Ellucian Portal		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Ellucian Workflow		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Ellucian PowerCampus		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Emerson	K-Series Coriolis Transmitters		Not Affected		Emerson Security Notification MR.RMT21003-2			12/17/2021
Emerson	Prolink Configuration Software		Not Affected		Emerson Security Notification MR.RMT21003-2			12/17/2021
Emerson	Prolink Mobile Application & ProcessViz Software		Not Affected		Emerson Security Notification MR.RMT21003-2			12/17/2021
Emerson	4732 Endeavor		Not Affected		Emerson Security Notification MR.RMT21003-2			12/17/2021
Emerson	Vortex and Magmeter Transmitters		Not Affected		Emerson Security Notification MR.RMT21003-2			12/17/2021
Emerson	USM 3410 and 3810 Series Ultrasonic Transmitters		Not Affected		Emerson Security Notification MR.RMT21003-2			12/17/2021
Emerson	Mark III Gas and Liquid USM		Not Affected		Emerson Security Notification MR.RMT21003-2			12/17/2021
Emerson	Flarecheck FlowCheck Flowel & PWAM software		Not Affected		Emerson Security Notification MR.RMT21003-2			12/17/2021
Emerson	MPFM2600 & MPFM5726		Not Affected		Emerson Security Notification MR.RMT21003-2			12/17/2021
Emerson	DHNC1 DHNC2		Not Affected		Emerson Security Notification MR.RMT21003-2			12/17/2021
Emerson	WCM SWGM		Not Affected		Emerson Security Notification MR.RMT21003-2			12/17/2021
Emerson	Fieldwatch and Service consoles		Not Affected		Emerson Security Notification MR.RMT21003-2			12/17/2021
Emerson	5726 Transmitter		Not Affected		Emerson Security Notification MR.RMT21003-2			12/17/2021
Emerson	Plantweb Advisor for Metrology and Metering Suite SDK		Not Affected		Emerson Security Notification MR.RMT21003-2			12/17/2021
Emerson	Gas Chromatographs: M500/2350A MON2000 700XA/1500XA 370XA MON2020		Not Affected		Emerson Security Notification MR.RMT21003-2			12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Emerson	Gas Analysis: X-STREAM Enhanced (XEGP XEGK XEGC XEGF XEFD XECLD)		Not Affected		Emerson Security Notification MR.RMT21003-2			12/17/2021
Emerson	Gas Detection: Millennium II Basic Single & Dual Channel 928 Wireless Gas Monitor/628 Gas Sensor 935 & 936 Open Path Gas Detector Millennium Air Particle Monitor		Not Affected		Emerson Security Notification MR.RMT21003-2			12/17/2021
Emerson	K-Series Coriolis Transmitters		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Prolink Configuration Software		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Prolink Mobile Application & ProcessViz Software		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	4732 Endeavor		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Vortex and Magmeter Transmitters		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	USM 3410 and 3810 Series Ultrasonic Transmitters		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Mark III Gas and Liquid USM		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Flarecheck FlowCheck Flowel & PWAM software		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	MPFM2600 & MPFM5726		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	DHNC1 DHNC2		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	WCM SWGM		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Fieldwatch and Service consoles		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	5726 Transmitter		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Plantweb Advisor for Metrology and Metering Suite SDK		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Emerson	Gas Chromatographs: M500/2350A MON2000 700XA/1500XA 370XA MON2020		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Gas Analysis: X-STREAM Enhanced (XEGP XEGK XEGC XEGF XEFD XECLD)		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Gas Detection: Millennium II Basic Single & Dual Channel 928 Wireless Gas Monitor/628 Gas Sensor 935 & 936 Open Path Gas Detector Millennium Air Particle Monitor		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Incus Ultrasonic gas leak detector		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Flame Detection: 975UF & 975UR Infrared Flame Detectors 975HR Infrared Hydrogen Flame Detector 975MR Multi-Spectrum Infrared Flame Detector		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Liquid Transmitters: 5081 1066 1056 1057 56		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Combustion: OCX OXT 6888 CX1100 6888Xi		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Spectrex family Flame Detectors and Rosemount 975 flame detector		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	CT4400 QCL General Purpose Continuous Gas Analyzer		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	CT5400 QCL General Purpose Continuous Gas Analyzer		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	CT5100 QCL Field Housing Continuous Gas Analyzer		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Emerson	CT5800 QCL Flameproof Housing Continuous Gas Analyzer		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	CT4215 QCL Packaging Leak Detection System		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	CT2211 QCL Aerosol Microleak Detection System		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	CT4404 QCL pMDI Leak Detection Analyzer		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	CT4000 QCL Marine OEM Gas Analyzer		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	CT3000 QCL Automotive OEM Gas Analyzer		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	3051 & 3051S Pressure transmitter families		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	2051 Pressure Transmitter Family		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	4088 Pressure Transmitter		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	2088 Pressure Transmitter Family		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	2090F/2090P Pressure Transmitters		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	4600 Pressure Transmitter		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	215 Pressure Sensor Module		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	550 PT Pressure Transmitter		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	326P Pressure Transmitter		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	3144P Temperature Transmitter		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	644 Temperature Transmitter		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	848T Temperature Transmitter		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	148 Temperature Transmitter		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	248 Temperature Transmitter		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Emerson	326T Temperature Transmitter		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	327T Temperature Transmitter		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	648 Temperature Transmitter		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	4088 Upgrade Utility		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Engineering Assistant 5.x & 6.x		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	248 Configuration Application		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Rosemount IO-Link Assistant		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Rosemount TankMaster and TankMaster Mobile		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Rosemount RadarMaster and RadarMaster Plus		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Rosemount Radar Configuration Tool		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Rosemount 2460 System Hub		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Rosemount 2410 Tank Hub		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Rosemount 3490 Controller		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Rosemount 2230 Graphical Field Display		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Rosemount 2240S Multi-input Temperature Transmitter		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Rosemount CMS/SCU 51/SCC		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Rosemount CMS/WSU 51/SWF 51		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Rosemount CMS/IOU 61		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Rosemount Level Transmitters (14xx 33xx 53xx 54xx 56xx)		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Emerson	Rosemount Radar Level Gauges (Pro 39xx 59xx)		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Rosemount Tank Radar Gauges (TGUxx)		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Rosemount Level Detectors (21xx)		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Emerson Aperio software		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
EnterpriseDT					EnterpriseDT Statement			
ESET					ESET Statement			
ESRI	ArcGIS Data Store	All	Fixed	Yes	https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/arcgis-software-and-cve-2021-44228-aka-log4shell-aka-logjam/	Requires script remediation. ESRI has created scripts to remove the JndiLookup class, but has not issued patches to upgrade the Log4j versions		12/17/2021
ESRI	ArcGIS Enterprise	All	Fixed	Yes	https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/arcgis-software-and-cve-2021-44228-aka-log4shell-aka-logjam/	Requires script remediation. ESRI has created scripts to remove the JndiLookup class, but has not issued patches to upgrade the Log4j versions		12/17/2021
ESRI	ArcGIS GeoEvent Server	All	Fixed	Yes	https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/arcgis-software-and-cve-2021-44228-aka-log4shell-aka-logjam/	Requires script remediation. ESRI has created scripts to remove the JndiLookup class, but has not issued patches to upgrade the Log4j versions		12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
ESRI	ArcGIS Server	All	Fixed	Yes	https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/arcgis-software-and-cve-2021-44228-aka-log4shell-aka-logjam/	Requires script remediation. ESRI has created scripts to remove the JndiLookup class, but has not issued patches to upgrade the Log4j versions		12/17/2021
ESRI	ArcGIS Workflow Manager Server	All	Fixed	Yes	https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/arcgis-software-and-cve-2021-44228-aka-log4shell-aka-logjam/	Requires script remediation. ESRI has created scripts to remove the JndiLookup class, but has not issued patches to upgrade the Log4j versions		12/17/2021
ESRI	Portal for ArcGIS	All	Fixed	Yes	https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/arcgis-software-and-cve-2021-44228-aka-log4shell-aka-logjam/	Requires script remediation. ESRI has created scripts to remove the JndiLookup class, but has not issued patches to upgrade the Log4j versions		12/17/2021
Estos					Estos Support Statement			
Evolveum Midpoint					Evolveum Midpoint Statement			
Ewon					Ewon Statement			
Exabeam					Exabeam Statement	This advisory is available to customers only and has not been reviewed by CISA		
Exact					Exact Statement			
Exivity					Exivity Statement			
ExtraHop	Reveal(x)	<=8.4.6, <=8.5.3, <=8.6.4	Affected	Yes	ExtraHop Statement	Versions >8.4.7, >8.5.4, >8.6.5 and >=8.7 are fixed.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
eXtreme Hosting					eXtreme Hosting Statement			
Extreme Networks					Extreme Networks Statement			
Extron					Extron Statement			
F-Secure	Elements Connector		Affected	Yes	The Log4J Vulnerability (CVE-2021-44228) – which F-Secure products are affected, what it means, what steps should you take - F-Secure Community			
F-Secure	Endpoint Proxy	13-15	Affected	Yes	F-Secure services Status - 0-day exploit found in the Java logging package log4j2			
F-Secure	Messaging Security Gateway		Affected	Yes	The Log4J Vulnerability (CVE-2021-44228) – which F-Secure products are affected, what it means, what steps should you take - F-Secure Community			
F-Secure	Policy Manager	13-15	Affected	Yes	F-Secure services Status - 0-day exploit found in the Java logging package log4j2			
F-Secure	Policy Manager Proxy	13-15	Affected	Yes	F-Secure services Status - 0-day exploit found in the Java logging package log4j2			
F5	BIG-IP (all modules)	11.x - 16.x	Not Affected		F5 Security Advisory			
F5	BIG-IQ Centralized Management	7.x-8.x	Not Affected		F5 Security Advisory			
F5	F5OS	1.x	Not Affected		F5 Security Advisory			
F5	Traffix SDC	5.x (5.2.0 CF1, 5.1.0 CF-30 - 5.1.0 CF-33)	Affected	No	F5 Security Advisory	Vulnerable components: EMS-ELK components (Fluentd + Elastic Search + Kibana), Element Management System		
F5	NGINX Plus	R19 - R25	Not Affected		F5 Security Advisory (CVE-2021-44228), F5 Security Advisory (CVE-2021-45046)			
F5	NGINX Open Source	1.x	Not Affected		F5 Security Advisory (CVE-2021-44228), F5 Security Advisory (CVE-2021-45046)			
F5	NGINX Unit	1.x	Not Affected		F5 Security Advisory (CVE-2021-44228), F5 Security Advisory (CVE-2021-45046)			
F5	NGINX App Protect	3.x	Not Affected		F5 Security Advisory (CVE-2021-44228), F5 Security Advisory (CVE-2021-45046)			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
F5	NGINX Controller	3.x	Not Affected		F5 Security Advisory (CVE-2021-44228), F5 Security Advisory (CVE-2021-45046)			
F5	NGINX Ingress Controller	1.x - 2.x	Not Affected		F5 Security Advisory (CVE-2021-44228), F5 Security Advisory (CVE-2021-45046)			
F5	NGINX Instance Manager	1.x	Not Affected		F5 Security Advisory (CVE-2021-44228), F5 Security Advisory (CVE-2021-45046)			
F5	NGINX Service Mesh	1.x	Not Affected		F5 Security Advisory (CVE-2021-44228), F5 Security Advisory (CVE-2021-45046)			
FAST LTA					FAST LTA Statement			
Fastly					Fastly Statement			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
FedEx	Ship Manager Software	Unknown	Affected/Under Investigation		FedEx Statement	Note: FedEx is aware of the issue related to the Log4j Remote Code Execution vulnerability affecting various Apache products. We are actively assessing the situation and taking necessary action as appropriate. As a result, we are temporarily unable to provide a link to download the FedEx Ship Manager software or generate product keys needed for registration of FedEx Ship Manager software. We are working to have this resolved as quickly as possible and apologize for the inconvenience. For related questions or the most updated information, customers should check FedEx Updates for Apache Log4j Issue or contact their Customer Technology representative.		12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Fiix	Fiix CMMS Core	v5	Fixed		PN1579 - Log4Shell Vulnerability Notice	The product has been updated to Log4j version 2.15. An additional patch is being developed to update to 2.16. No user interaction is required.		12/15/2021
FileCap					FileCapStatement			
FileCatalyst					FileCatalyst Statement			
FileCloud					FileCloud Statement			
FileWave					FileWave Statement			
FINVI					FINVI Statement			
FireDaemon					FireDemon Statement			
Fisher & Paykel Healthcare			Not Affected		Fisher & Paykel Healthcare Advisory Link			12/21/2021
Flexagon					Flexagon Statement			
Flexera					Flexera Statement			
Forcepoint	DLP Manager		Affected		Login (forcepoint.com)			
Forcepoint	Forcepoint Cloud Security Gateway (CSG)		Not Affected		Login (forcepoint.com)			
Forcepoint	Next Generation Firewall (NGFW)		Not Affected		Login (forcepoint.com)			
Forcepoint	Next Generation Firewall, NGFW VPN Client, Forcepoint User ID service and Sidewinder		Not Affected		Login (forcepoint.com)			
Forcepoint	One Endpoint		Not Affected		Login (forcepoint.com)			
Forcepoint	Security Manager (Web, Email and DLP)		Affected		Login (forcepoint.com)			
Forescout					Forescout Statement			
ForgeRock	Autonomous Identity		Affected		Security Advisories - Knowledge - BackStage (forgerock.com)	all other ForgeRock products Not vulnerable		
Fortinet	FortiAIOps		Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiAnalyzer		Not Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiAnalyzer Cloud		Not Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiAP		Not Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiAuthenticator		Not Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiCASB		Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiConvertor		Affected		PSIRT Advisories FortiGuard			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Fortinet	FortiDeceptor		Not Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiEDR Agent		Not Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiEDR Cloud		Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiGate Cloud		Not Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiGSLB Cloud		Not Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiMail		Not Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiManager		Not Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiManager Cloud		Not Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiNAC		Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiNAC		Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiOS (includes FortiGate & FortiWiFi)		Not Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiPhish Cloud		Not Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiPolicy		Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiPortal		Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiRecorder		Not Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiSIEM		Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiSOAR		Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiSwicth Cloud in FortiLANCloud		Not Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiSwitch & FortiSwitchManager		Not Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiToken Cloud		Not Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiVoice		Not Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiWeb Cloud		Not Affected		PSIRT Advisories FortiGuard			
Fortinet	ShieldX		Affected		PSIRT Advisories FortiGuard			
FTAPI					FTAPI Statement			
Fujitsu					Fujitsu Statement			
FusionAuth	FusionAuth	1.32	Not Affected		log4j CVE: How it affects FusionAuth (TLDR: It doesn't) - FusionAuth			
GE Digital			Unknown		GE Digital Advisory Link(login required)	This advisory is available to customers only and has not been reviewed by CISA.		12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
GE Digital Grid			Unknown		GE Digital Grid Advisory Link(login required)	This advisory is available to customers only and has not been reviewed by CISA.		12/22/2021
GE Gas Power	Baseline Security Center (BSC)		Affected		GE Gas Power Advisory Link	Vulnerability to be fixed by vendor provided workaround. No user actions necessary. Contact GE for details.		12/22/2021
GE Gas Power	Baseline Security Center (BSC) 2.0		Affected		GE Gas Power Advisory Link	Vulnerability to be fixed by vendor provided workaround. No user actions necessary. Contact GE for details		12/22/2021
GE Gas Power	Asset Performance Management (APM)		Affected		GE Gas Power Advisory Link	GE verifying workaround.		12/22/2021
GE Gas Power	Control Server		Affected		GE Gas Power Advisory Link	The Control Server is Affected via vCenter. There is a fix for vCenter. Please see below. GE verifying the vCenter fix as proposed by the vendor.		12/22/2021
GE Gas Power	Tag Mapping Service		Affected	Yes	GE Gas Power Advisory Link	Vulnerability fixed. No user actions necessary. Updated to log4j 2.16		12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
GE Healthcare			Unknown		GE Healthcare Advisory Link	This advisory is not available at the time of this review, due to maintence on the GE Healthcare website.		12/22/2021
Gearset					Gearset Statement			
Genesys					Genesys Statement			
GeoServer					GeoServer Announcement			
Gerrit code review					Gerrit Statement			
GFI					GFI Statement			
Ghidra					Ghidra Statement			
Gigamon	Fabric Manager	<5.13.01.02	Affected	Yes	Gigamon Customer Support Portal	Updates available via the Gigamon Support Portal. This advisory available to customers only and has not been reviewed by CISA.		12/21/2021
GitHub	GitHub	GitHub.com and GitHub Enterprise Cloud	Fixed		GitHub Statement			12/17/2021
GitLab					GitLab Statement			
Globus					Globus Statement			
GoAnywhere	MFT	< 6.8.6	Affected	Yes	GoAnywhere Statement			12/18/2021
GoAnywhere	Gateway	< 2.8.4	Affected	Yes	GoAnywhere Statement			12/18/2021
GoAnywhere	MFT Agents	< 1.6.5	Affected	Yes	GoAnywhere Statement			12/18/2021
GoCD					GoCD Statement			
Google Cloud	AI Platform Data Labeling		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	AI Platform Neural Architecture Search (NAS)		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	AI Platform Training and Prediction		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Access Transparency		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Actifio		Not Affected		https://cloud.google.com/log4j2-security-advisory	Actifio has identified limited exposure to the Log4j 2 vulnerability and has released a hotfix to address this vulnerability. Visit https://now.actifio.com for the full statement and to obtain the hotfix (available to Actifio customers only).		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Anthos		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046. Customers may have introduced a separate logging solution that uses Log4j 2. We strongly encourage customers who manage Anthos environments to identify components dependent on Log4j 2 and update them to the latest version.		12/21/2021
Google Cloud	Anthos Config Management		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Anthos Connect		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Anthos Hub		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Anthos Identity Service		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Anthos Premium Software		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Anthos Service Mesh		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Anthos on VMWare		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046. We strongly encourage customers to check VMware recommendations documented in VMSA-2021-0028 and deploy fixes or workarounds to their VMware products as they become available. We also recommend customers review their respective applications and workloads affected by the same vulnerabilities and apply appropriate patches.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Apigee		Not Affected		https://cloud.google.com/log4j2-security-advisory	Apigee installed Log4j 2 in its Apigee Edge VMs, but the software was not used and therefore the VMs were not impacted by the issues in CVE-2021-44228 and CVE-2021-45046. Apigee updated Log4j 2 to v.2.16 as an additional precaution. It is possible that customers may have introduced custom resources that are using vulnerable versions of Log4j. We strongly encourage customers who manage Apigee environments to identify components dependent on Log4j and update them to the latest version. Visit the Apigee Incident Report for more information.		12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	App Engine		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046. Customers may have introduced a separate logging solution that uses Log4j 2. We strongly encourage customers who manage App Engine environments to identify components dependent on Log4j 2 and update them to the latest version.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	AppSheet		Not Affected		https://cloud.google.com/log4j2-security-advisory	The AppSheet core platform runs on non-JVM (non-Java) based runtimes. At this time, we have identified no impact to core AppSheet functionality. Additionally, we have patched one Java-based auxiliary service in our platform. We will continue to monitor for affected services and patch or remediate as required. If you have any questions or require assistance, contact AppSheet Support.		12/21/2021
Google Cloud	Artifact Registry		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Assured Workloads		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	AutoML		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	AutoML Natural Language		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	AutoML Tables		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	AutoML Translation		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	AutoML Video		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	AutoML Vision		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	BigQuery		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	BigQuery Data Transfer Service		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	BigQuery Omni		Not Affected		https://cloud.google.com/log4j2-security-advisory	BigQuery Omni, which runs on AWS and Azure infrastructure, does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046. We continue to work with AWS and Azure to assess the situation.		12/19/2021
Google Cloud	Binary Authorization		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Certificate Manager		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Chronicle		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/20/2021
Google Cloud	Cloud Asset Inventory		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Cloud Bigtable		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/19/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Cloud Build		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046. Customers may have introduced a separate logging solution that uses Log4j 2. We strongly encourage customers who manage Cloud Build environments to identify components dependent on Log4j 2 and update them to the latest version.		12/21/2021
Google Cloud	Cloud CDN		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/20/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Cloud Composer		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046. Cloud Composer does not use Log4j 2 and is not impacted by the issues in CVE-2021-44228 and CVE-2021-45046. It is possible that customers may have imported or introduced other dependencies via DAGs, installed PyPI modules, plugins, or other services that are using vulnerable versions of Log4j 2. We strongly encourage customers, who manage Composer environments to identify components dependent on Log4j 2 and update them to the latest version.		12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Cloud Console App		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Cloud DNS		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/20/2021
Google Cloud	Cloud Data Loss Prevention		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Cloud Debugger		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Cloud Deployment Manager		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Cloud Endpoints		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Cloud External Key Manager (EKM)		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Cloud Functions		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046. Customers may have introduced a separate logging solution that uses Log4j 2. We strongly encourage customers who manage Cloud Functions environments to identify components dependent on Log4j 2 and update them to the latest version.		12/21/2021
Google Cloud	Cloud Harware Security Module (HSM)		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Cloud Intrusion Detection System (IDS)		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Cloud Interconnect		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Cloud Key Management Service		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Cloud Load Balancing		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/20/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Cloud Logging		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Cloud Network Address Translation (NAT)		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/20/2021
Google Cloud	Cloud Natural Language API		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Cloud Profiler		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Cloud Router		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/20/2021
Google Cloud	Cloud Run		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046. Customers may have introduced a separate logging solution that uses Log4j 2. We strongly encourage customers who manage Cloud Run environments to identify components dependent on Log4j 2 and update them to the latest version.		12/21/2021		
Google Cloud	Cloud Run for Anthos		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046. Customers may have introduced a separate logging solution that uses Log4j 2. We strongly encourage customers who manage Cloud Run for Anthos environments to identify components dependent on Log4j 2 and update them to the latest version.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Cloud SDK		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Cloud SQL		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/19/2021
Google Cloud	Cloud Scheduler		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Cloud Shell		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046. Customers may have introduced a separate logging solution that uses Log4j 2. We strongly encourage customers who manage Cloud Shell environments to identify components dependent on Log4j 2 and update them to the latest version.		12/21/2021
Google Cloud	Cloud Source Repositories		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Cloud Spanner		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/19/2021
Google Cloud	Cloud Storage		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/20/2021
Google Cloud	Cloud Tasks		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Cloud Trace		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Cloud Traffic Director		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/20/2021
Google Cloud	Cloud Translation		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Cloud VPN		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/20/2021
Google Cloud	Cloud Vision		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Cloud Vision OCR On-Prem		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	CompilerWorks		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/20/2021
Google Cloud	Compute Engine		Not Affected		https://cloud.google.com/log4j2-security-advisory	Compute Engine does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046. For those using Google Cloud VMware Engine, we are working with VMware and tracking VMSA-2021-0028.1. We will deploy fixes to Google Cloud VMware Engine as they become available.		12/20/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Contact Center AI (CCAI)		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Contact Center AI Insights		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Container Registry		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Data Catalog		Not Affected		https://cloud.google.com/log4j2-security-advisory	Data Catalog has been updated to mitigate the issues identified in CVE-2021-44228 and CVE-2021-45046. We strongly encourage customers who introduced their own connectors to identify dependencies on Log4j 2 and update them to the latest version.		12/20/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Data Fusion		Not Affected		https://cloud.google.com/log4j2-security-advisory	Data Fusion does not use Log4j 2, but uses Dataproc as one of the options to execute pipelines. Dataproc released new images on December 18, 2021 to address the vulnerability in CVE-2021-44228 and CVE-2021-45046. Customers must follow instructions in a notification sent on December 18, 2021 with the subject line “Important information about Data Fusion.”		12/20/2021
Google Cloud	Database Migration Service (DMS)		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/19/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Dataflow		Not Affected		https://cloud.google.com/log4j2-security-advisory	Dataflow does not use Log4j 2 and is not impacted by the issues in CVE-2021-44228 and CVE-2021-45046. If you have changed dependencies or default behavior, it is strongly recommended you verify there is no dependency on vulnerable versions Log4j 2. Customers have been provided details and instructions in a notification sent on December 17, 2021 with the subject line "Update #1 to Important information about Dataflow."		12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Dataproc		Not Affected		https://cloud.google.com/log4j2-security-advisory	Dataproc released new images on December 18, 2021 to address the vulnerabilities in CVE-2021-44228 and CVE-2021-45046. Customers must follow the instructions in notifications sent on December 18, 2021 with the subject line “Important information about Dataproc” with Dataproc documentation.		12/20/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Dataproc Metastore		Not Affected		https://cloud.google.com/log4j2-security-advisory	Dataproc Metastore has been updated to mitigate the issues identified in CVE-2021-44228 and CVE-2021-45046. Customers who need to take actions were sent two notifications with instructions on December 17, 2021 with the subject line “Important information regarding Log4j 2 vulnerability in your gRPC-enabled Dataproc Metastore.”		12/20/2021
Google Cloud	Datastore		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/19/2021
Google Cloud	Datastream		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/19/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Dialogflow Essentials (ES)		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Document AI		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Event Threat Detection		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Eventarc		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Filestore		Not Affected		https://cloud.google.com/log4j2-security-advisory	Log4j 2 is contained within the Filestore service; there is a technical control in place that mitigates the vulnerabilities in CVE-2021-44228 and CVE-2021-45046. Log4j 2 will be updated to the latest version as part of the scheduled rollout in January 2022.		12/21/2021
Google Cloud	Firebase		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Firestore		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/19/2021
Google Cloud	Game Servers		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Google Cloud Armor		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/20/2021
Google Cloud	Google Cloud Armor Managed Protection Plus		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/20/2021
Google Cloud	Google Cloud VMware Engine		Not Affected		https://cloud.google.com/log4j2-security-advisory	We are working with VMware and tracking VMSA-2021-0028.1. We will deploy fixes as they become available.		12/11/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Google Kubernetes Engine		Not Affected		https://cloud.google.com/log4j2-security-advisory	Google Kubernetes Engine does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046. Customers may have introduced a separate logging solution that uses Log4j 2. We strongly encourage customers who manage Google Kubernetes Engine environments to identify components dependent on Log4j 2 and update them to the latest version.		12/21/2021
Google Cloud	Healthcare Data Engine (HDE)		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Human-in-the-Loop AI		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	IoT Core		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Key Access Justifications (KAJ)		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Looker		Not Affected		https://cloud.google.com/log4j2-security-advisory	Looker-hosted instances have been updated to a Looker version with Log4j v2.16. Looker is currently working with third-party driver vendors to evaluate the impact of the Log4j vulnerability. As Looker does not enable logging for these drivers in Looker-hosted instances, no messages are logged. We conclude that the vulnerability is mitigated. We continue to actively work with the vendors to deploy a fix for these drivers. Looker customers who self-manage their Looker instances have received instructions through their technical contacts on how to take the necessary steps to address the vulnerability. Looker customers who have questions or require assistance, please visit Looker Support.		12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Media Translation API		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Memorystore		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/19/2021
Google Cloud	Migrate for Anthos		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Migrate for Compute Engine (M4CE)		Not Affected		https://cloud.google.com/log4j2-security-advisory	M4CE has been updated to mitigate the issues identified in CVE-2021-44228 and CVE-2021-45046. M4CE has been updated to version 4.11.9 to address the vulnerabilities. A notification was sent to customers on December 17, 2021 with subject line "Important information about CVE-2021-44228 and CVE-2021-45046" for M4CE V4.11 or below. If you are on M4CE v5.0 or above, no action is needed.		12/19/2021
Google Cloud	Network Connectivity Center		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/20/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Network Intelligence Center		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/20/2021
Google Cloud	Network Service Tiers		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/20/2021
Google Cloud	Persistent Disk		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/20/2021
Google Cloud	Pub/Sub		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/16/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Pub/Sub Lite		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046. Customers may have introduced a separate logging solution that uses Log4j 2. We strongly encourage customers who manage Pub/Sub Lite environments to identify components dependent on Log4j 2 and update them to the latest version.		12/16/2021
Google Cloud	reCAPTCHA Enterprise		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Recommendations AI		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Retail Search		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Risk Manager		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Secret Manager		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Security Command Center		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Service Directory		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Service Infrastructure		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Speaker ID		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Speech-to-Text		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Speech-to-Text On-Prem		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Storage Transfer Service		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/20/2021
Google Cloud	Talent Solution		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Text-to-Speech		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Transcoder API		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Transfer Appliance		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Video Intelligence API		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Virtual Private Cloud		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/20/2021
Google Cloud	Web Security Scanner		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Workflows		Not Affected		https://cloud.google.com/log4j2-security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Gradle	Gradle		Not Affected	No	Gradle Blog - Dealing with the critical Log4j vulnerability	Gradle Scala Compiler Plugin depends upon log4j-core but it is not used.		
Gradle	Gradle Enterprise	< 2021.3.6	Affected	Yes	Gradle Enterprise Security Advisories - Remote code execution vulnerability due to use of Log4j2			
Gradle	Gradle Enterprise Build Cache Node	< 10.1	Affected	Yes	Gradle Enterprise Security Advisories - Remote code execution vulnerability due to use of Log4j2			
Gradle	Gradle Enterprise Test Distribution Agent	< 1.6.2	Affected	Yes	Gradle Enterprise Security Advisories - Remote code execution vulnerability due to use of Log4j2			
Grafana					Grafana Statement			
Grandstream					Grandstream Statement			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Gravitee	Access Management	3.10.x	Not Affected	No	About the Log4J CVSS 10 Critical Vulnerability			
Gravitee	Access Management	3.5.x	Not Affected	No	About the Log4J CVSS 10 Critical Vulnerability			
Gravitee	API Management	3.10.x	Not Affected	No	About the Log4J CVSS 10 Critical Vulnerability			
Gravitee	API Management	3.5.x	Not Affected	No	About the Log4J CVSS 10 Critical Vulnerability			
Gravitee	Alert Engine	1.5.x	Not Affected	Yes	About the Log4J CVSS 10 Critical Vulnerability			
Gravitee	Alert Engine	1.4.x	Not Affected	No	About the Log4J CVSS 10 Critical Vulnerability			
Gravitee	Cockpit	1.4.x	Not Affected	No	About the Log4J CVSS 10 Critical Vulnerability			
Gravitee.io					Gravitee.io Statement			
Gravwell					Gravwell Statement			
Graylog	Graylog Server	All versions >= 1.2.0 and <= 4.2.2	Affected	Yes	Graylog Update for Log4j			
GreenShot					GreenShot Statement			
Guidewire					Guidewire Statement			
HAProxy					HAProxy Statement			
HarmanPro AMX					HarmanPro AMX Statement			
HashiCorp	Boundary		Not Affected		HashiCorp security bulletin re. CVE-2021-44228			
HashiCorp	Consul		Not Affected		HashiCorp security bulletin re. CVE-2021-44228			
HashiCorp	Consul Enterprise		Not Affected		HashiCorp security bulletin re. CVE-2021-44228			
HashiCorp	Nomad		Not Affected		HashiCorp security bulletin re. CVE-2021-44228			
HashiCorp	Nomad Enterprise		Not Affected		HashiCorp security bulletin re. CVE-2021-44228			
HashiCorp	Packer		Not Affected		HashiCorp security bulletin re. CVE-2021-44228			
HashiCorp	Terraform		Not Affected		HashiCorp security bulletin re. CVE-2021-44228			
HashiCorp	Terraform Enterprise		Not Affected		HashiCorp security bulletin re. CVE-2021-44228			
HashiCorp	Vagrant		Not Affected		HashiCorp security bulletin re. CVE-2021-44228			
HashiCorp	Vault		Not Affected		HashiCorp security bulletin re. CVE-2021-44228			
HashiCorp	Vault Enterprise		Not Affected		HashiCorp security bulletin re. CVE-2021-44228			
HashiCorp	Waypoint		Not Affected		HashiCorp security bulletin re. CVE-2021-44228			
HCL Software	BigFix Compliance	2.0.1 - 2.0.4	Fixed		KB with fix	Not Affected for related CVE-2021-45046	Forum post with more specifics	12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HCL Software	BigFix Insights	All	Not Affected		KB	Not Affected for related CVE-2021-45046		12/15/2021
HCL Software	BigFix Insights for Vulnerability Remediation	All	Not Affected		KB	Not Affected for related CVE-2021-45046		12/15/2021
HCL Software	BigFix Inventory	< 10.0.7	Fixed		KB with fix	Not Affected for related CVE-2021-45046		12/15/2021
HCL Software	BigFix Lifecycle	All	Not Affected		KB	Not Affected for related CVE-2021-45046		12/15/2021
HCL Software	BigFix Mobile	All	Not Affected		KB	Not Affected for related CVE-2021-45046		12/15/2021
HCL Software	BigFix Patch	All	Not Affected		KB	Not Affected for related CVE-2021-45046		12/15/2021
HelpSystems Clearswift					HelpSystems Clearswift			
HENIX	Squash TM	1.21.7 - 1.22.9, 2.0.3 - 2.1.5, 2.2.0 - 3.0.2	Fixed		Vendor Link			12/23/2021
Hexagon					Hexagon Statement			
Hikvision					Hikvision			
Hitachi Energy	eSOMS		Not Affected		Hitachi Energy			
Hitachi Vantara					Hitachi Vantara			
Honeywell					Honeywell Statement			
HP	Teradici Cloud Access Controller	< v113	Fixed	Yes	Apache Log4j update for Teradici PCoIP Connection Manager, Teradici Cloud Access Connector, Teradici PCoIP License Server, Teradici Management Console, and Teradici EMSDK			2021-12-17
HP	Teradici EMSDK	< 1.0.6	Fixed	Yes	Apache Log4j update for Teradici PCoIP Connection Manager, Teradici Cloud Access Connector, Teradici PCoIP License Server, Teradici Management Console, and Teradici EMSDK			2021-12-17
HP	Teradici Management Console	< 21.10.3	Fixed	Yes	Apache Log4j update for Teradici PCoIP Connection Manager, Teradici Cloud Access Connector, Teradici PCoIP License Server, Teradici Management Console, and Teradici EMSDK			2021-12-17

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HP	Teradici PCoIP Connection Manager	< 21.03.6, < 20.07.4	Fixed	Yes	Apache Log4j update for Teradici PCoIP Connection Manager, Teradici Cloud Access Connector, Teradici PCoIP License Server, Teradici Management Console, and Teradici EMSDK			2021-12-17
HP	Teradici PCoIP License Server		Not Affected		Apache Log4j update for Teradici PCoIP Connection Manager, Teradici Cloud Access Connector, Teradici PCoIP License Server, Teradici Management Console, and Teradici EMSDK			2021-12-17
HPE	3PAR StoreServ Arrays		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	AirWave Management Platform		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Alletra 6000		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Alletra 9k		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Aruba Central		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Aruba ClearPass Policy Manager		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Aruba ClearPass Policy Manager		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	Aruba Instant (IAP)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Aruba Location Services		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Aruba NetEdit		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Aruba PVOS Switches		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Aruba SDN VAN Controller		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Aruba User Experience Insight (UXI)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Aruba VIA Client		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	ArubaOS-CX switches		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	ArubaOS-S switches		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	ArubaOS SD-WAN Controllers and Gateways		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	ArubaOS Wi-Fi Controllers and Gateways		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	BladeSystem Onboard Administrator		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Brocade 16Gb Fibre Channel SAN Switch for HPE Synergy		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Brocade 16Gb SAN Switch for HPE BladeSystem c-Class		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Brocade 32Gb Fibre Channel SAN Switch for HPE Synergy		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Brocade Network Advisor		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	CloudAuth		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	CloudPhysics		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	Compute Cloud Console		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Compute operations manager- FW UPDATE SERVICE		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	COS (Cray Operating System)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Cray Systems Management (CSM)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Custom SPP Portal Link		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Data Services Cloud Console		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Harmony Data Platform		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HOP public services (grafana, vault, rancher, Jenkins)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HPE B-series SN2600B SAN Extension Switch		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	HPE B-series SN4000B SAN Extension Switch		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HPE B-series SN6000B Fibre Channel Switch		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HPE B-series SN6500B Fibre Channel Switch		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HPE B-series SN6600B Fibre Channel Switch		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HPE B-series SN6650B Fibre Channel Switch		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HPE B-series SN6700B Fibre Channel Switch		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HPE Customer Experience Assurance (CEA)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE Hardware Support Manager plug-in for VMware vSphere Lifecycle Manager		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HPE Home Location Register (HLR/I-HLR)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	HPE Infosight for Servers		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HPE Integrated Home Subscriber Server (I-HSS)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE Intelligent Messaging (IM)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE Intelligent Network Server (INS)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE Multimedia Services Environment (MSE)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE OC Convergent Communications Platform (OCCP)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE OC Media Platform Media Resource Function (OCMP-MRF)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE OC Service Access Controller (OC SAC)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE OC Service Controller (OCSC)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	HPE OC Universal Signaling Platform (OC-USP-M)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE OneView		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HPE OneView for VMware vRealize Operations (vROps)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HPE OneView Global Dashboard		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HPE Performance Cluster Manager (HPCM)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE Performance Manager (PM)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE Position Determination Entity (PDE)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE Secure Identity Broker (SIB)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE Service Activator (SA)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	HPE Service Governance Framework (SGF)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE Service Orchestration Manager (SOM)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE Service Provisioner (SP)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE Short Message Point-to-Point Gateway (SMPP)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE Slingshot		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HPE Smart Interaction Server (SIS)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE SN3000B Fibre Channel Switch		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HPE SN8000B 4-Slot SAN Director Switch		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HPE SN8000B 8-Slot SAN Backbone Director Switch		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	HPE SN8600B 4-Slot SAN Director Switch		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HPE SN8600B 8-Slot SAN Director Switch		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HPE SN8700B 4-Slot Director Switch		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HPE SN8700B 8-Slot Director Switch		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HPE Subscriber, Network, and Application Policy (SNAP)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE Subscription Manager (SM)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE Synergy Image Streamer		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HPE Systems Insight Manager (SIM)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HPE Telecom Application Server (TAS)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	HPE Unified Correlation and Automation (UCA)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE Unified Mediation Bus (UMB)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE Unified OSS Console (UOC)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE Unified Topology Manager (UTM)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE Universal Identity Repository (VIR)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE Universal SLA Manager (uSLAM)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE Virtual Connect		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HPE Virtual Connect Enterprise Manager (VCEM)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HPE Virtual Provisioning Gateway (vPGW)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	HPE Virtual Server Environment (VSE)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	HPE Virtual Subscriber Data Management (vSDM)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE WebRTC Gateway Controller (WGW)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-14
HPE	HPE Wi-Fi Authentication Gateway (WauG)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Insight Cluster Management Utility (CMU)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Integrated Lights-Out (iLO) Amplifier Pack		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Integrated Lights-Out 4 (iLO 4)	4	Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Integrated Lights-Out 5 (iLO 5)	5	Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Integrity BL860c, BL870c, BL890c		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	Integrity Rx2800/Rx2900		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Integrity Superdome 2		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Integrity Superdome X		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Intelligent Provisioning		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	iSUT integrated smart update tool		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Maven Artifacts (Atlas)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	MSA		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	NetEdit		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Nimble Storage		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	NS-T0634-OSM CONSOLE TOOLS		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	NS-T0977-SCHEMA VALIDATOR		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	OfficeConnect		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Primera Storage		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	RepoServer part of OPA (on Premises aggregator)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Resource Aggregator for Open Distributed Infrastructure Management		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	RESTful Interface Tool (iLOREST)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	SAT (System Admin Toolkit)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Scripting Tools for Windows PowerShell (HPEiLOCmdlets)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	SGI MC990 X Server		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	SGI UV 2000 Server		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	SGI UV 300, 300H, 300RL, 30EX		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	SGI UV 3000 Server		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	SN8700B 8-Slot Director Switch		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	StoreEasy		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	StoreEver CVTL		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	StoreEver LTO Tape Drives		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	StoreEver MSL Tape Libraries		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	StoreOnce		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	SUM (Smart Update Manager)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Superdome Flex 280		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	Superdome Flex Server		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HPE	UAN (User Access Node)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387		2021-12-12
HOLOGIC	Advanced Workflow Manager (AWM)		Affected	No	HOLOGIC Advisory Link	While the Hologic software itself does not utilize Java/Log4J, the installed APC PowerChute UPS with Business Edition v9.5 software installed may. APC is still assessing its PowerChute software to determine if it is vulnerable.		12/20/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HOLOGIC	Unifi Workspace		Affected	No	HOLOGIC Advisory Link	While the Hologic software itself does not utilize Java/Log4J, the installed APC PowerChute UPS with Business Edition v9.5 software installed may. APC is still assessing its PowerChute software to determine if it is vulnerable.		12/20/2021
HOLOGIC	Faxitron CT Specimen Radiography System		Affected	No	HOLOGIC Advisory Link	While the Hologic software itself does not utilize Java/Log4J, there is a utility program installed that may utilize Java and Log4J. This utility program does not run on startup and is not required for system operation. Please contact Hologic Service for assistance in removing this program.		12/20/2021
HOLOGIC	Dimensions / 3Dimensions Mammography System		Not Affected	No	HOLOGIC Advisory Link			12/20/2021
HOLOGIC	Affirm Prone Biopsy System		Not Affected	No	HOLOGIC Advisory Link			12/20/2021
HOLOGIC	Brevera Breast Biopsy System		Not Affected	No	HOLOGIC Advisory Link			12/20/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HOLOGIC	Trident HD Specimen Radiography System		Not Affected	No	HOLOGIC Advisory Link			12/20/2021
HOLOGIC	SecurView DX Workstation		Not Affected	No	HOLOGIC Advisory Link			12/20/2021
HOLOGIC	Cenova Image Analytics Server		Not Affected	No	HOLOGIC Advisory Link			12/20/2021
HOLOGIC	SecurXChange Router		Not Affected	No	HOLOGIC Advisory Link			12/20/2021
HOLOGIC	Rosetta DC Tomosynthesis Data Converter		Not Affected	No	HOLOGIC Advisory Link			12/20/2021
HOLOGIC	Faxitron Specimen Radiography Systems		Not Affected	No	HOLOGIC Advisory Link			12/20/2021
HOLOGIC	Horizon DXA Bone Densitometer		Not Affected	No	HOLOGIC Advisory Link			12/20/2021
HOLOGIC	Discovery Bone Densitometer		Not Affected	No	HOLOGIC Advisory Link			12/20/2021
HOLOGIC	Fluoroscan Insight Mini C-Arm		Not Affected	No	HOLOGIC Advisory Link			12/20/2021
HOLOGIC	SuperSonic Imagine Ultrasound Products (Aixplorer & Aixplorer Mach)		Not Affected	No	HOLOGIC Advisory Link			12/20/2021
HOLOGIC	Windows Selenia Mammography System		Not Affected	No	HOLOGIC Advisory Link			12/20/2021
Huawei					Huawei Security Notice			
Hubspot					Hubspot Notice			
I-Net software					I-Net Software Statement			
I2P					I2P Statement			
IBA-AG					IBA-AG Statement			
Ibexa					Ibexa Statement			
IBM	BigFix Compliance		Affected	No				
IBM	BigFix Inventory	VM Manager Tool & SAP Tool	Affected	No		To verify if your instance is affected, go to the lib subdirectory of the tool (BESClient/LMT/SAPTOOL and BESClient/LMT/VMMAN) and check what version of log4j is included. Version is included in the name of the library.		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	Analytics Engine		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	App Configuration		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	App Connect		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	App ID		Affected	Yes	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Application Gateway		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Aspera Endpoint		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Aspera Enterprise		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Aspera fasp.io		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Aspera		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Bare Metal Servers		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Block Storage		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Block Storage for VPC		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Block Storage Snapshots for VPC		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	Case Manager		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Certificate Manager		Affected	Yes	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Client VPN for VPC		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Cloud Activity Tracker		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Cloud Backup		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Cloud Monitoring		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Cloud Object Storage		Affected	Yes	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Cloud Object Storage		Affected	Yes	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Cloudant		Affected	Yes	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Code Engine		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Cognos Command Center		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Cognos Controller	10.4.2	Affected	Yes	Security Bulletin: IBM Cognos Controller 10.4.2 IF15: Apache log4j Vulnerability (CVE-2021-44228)			12/15/2021
IBM	Cognos Integration Server		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	Compose Enterprise		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Compose for Elasticsearch		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Compose for etcd		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Compose for MongoDB		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Compose for MySQL		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Compose for PostgreSQL		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Compose for RabbitMQ		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Compose for Redis		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Compose for RethinkDB		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Compose for ScyllaDB		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Container Registry		Affected	Yes	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Container Security Services		Affected	Yes	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Content Delivery Network		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	Continuous Delivery		Affected	Yes	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Copy Services Manager		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Databases for DataStax		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Databases for EDB		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Databases for Elasticsearch		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Databases for etcd		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Databases for MongoDB		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Databases for PostgreSQL		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Databases for Redis		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Datapower Gateway		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Dedicated Host for VPC		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Direct Link Connect		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Direct Link Connect on Classic		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	Direct Link Dedicated (2.0)		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Direct Link Dedicated Hosting on Classic		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Direct Link Dedicated on Classic		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Direct Link Exchange on Classic		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	DNS Services		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Emptoris Contract Management		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Emptoris Program Management		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Emptoris Sourcing		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Emptoris Spend Analysis		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Emptoris Supplier Lifecycle Management		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Enterprise Tape Controller Model C07 (3592) (ETC)		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Event Notifications		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Event Streams		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	File Storage		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Flash System 900 (& 840)		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Flow Logs for VPC		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Functions		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	GSKit		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Guardium S-TAP for Data Sets on z/OS		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Guardium S-TAP for DB2 on z/OS		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Guardium S-TAP for IMS on z/OS		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Hyper Protect Crypto Services		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Hyper Protect DBaaS for MongoDB		Affected	Yes	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Hyper Protect DBaaS for PostgreSQL		Affected	Yes	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Hyper Protect Virtual Server		Affected	Yes	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	i2 Analyst’s Notebook		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	i2 Base		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	IBM Application Runtime Expert for i		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	IBM Backup, Recovery and Media Services for i		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	IBM Db2 Mirror for i		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	IBM HTTP Server		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	IBM i Access Family		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	IBM i Portfolio of products under the Group SWMA		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	IBM PowerHA System Mirror for i		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	IBM Sterling Connect:Direct Browser User Interface		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	IBM Sterling Connect:Direct File Agent	See Vendor Links	Affected	Yes	Security Bulletin: Apache Log4j Vulnerability Affects IBM Sterling Connect:Direct for UNIX (CVE-2021-44228), An update on the Apache Log4j 2.x vulnerabilities		https://www.ibm.com/support/pages/node/6526688, https://www.ibm.com/support/pages/node/6528324, https://www.ibm.com/blogs/psirt/an-update-on-the-apache-log4j-cve-2021-44228-vulnerability/	12/20/2021
IBM	IBM Sterling Connect:Direct for HP NonStop		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	IBM Sterling Connect:Direct for i5/OS		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	IBM Sterling Connect:Direct for OpenVMS		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	IBM Sterling Connect:Express for Microsoft Windows		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	IBM Sterling Connect:Express for UNIX		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	IBM Sterling Connect:Express for z/OS		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Instana Agent	Timestamp lower than 12-11-2021	Affected	Yes	Status Instana			12/14/2021
IBM	Internet Services		Affected	Yes	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Key Lifecyle Manager for z/OS		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Key Protect		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Knowledge Studio		Affected	Yes	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Kubernetes Service		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Load Balancer for VPC		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Log Analysis		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Managed VMware Service		Affected	Yes	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Management Extender for VMware vCenter		Affected	No				

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	Mass Data Migration		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Maximo EAM SaaS		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Message Hub		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	MQ Appliance		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	MQ on IBM Cloud		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Natural Language Understanding		Affected	Yes	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	OmniFind Text Search Server for DB2 for i		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	OPENBMC		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Planning Analytics Workspace	>2.0.57	Affected	Yes	Security Bulletin: IBM Planning Analytics 2.0: Apache log4j Vulnerability (CVE-2021-44228)			12/15/2021
IBM	Power HMC	V9.2.950.0 & V10.1.1010.0	Affected	Yes	Security Bulletin: Vulnerability in Apache Log4j (CVE-2021-44228) affects Power HMC			12/15/2021
IBM	PowerSC		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	PowerVM Hypervisor		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	PowerVM VIOS		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	QRadar Advisor		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Qradar Network Threat Analytics		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	QRadar SIEM		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Quantum Services		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Rational Developer for AIX and Linux		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Rational Developer for i		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Red Hat OpenShift on IBM Cloud		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Resilient		Under Investigation					
IBM	Robotic Process Automation		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	SAN Volume Controller and Storwize Family		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Satellite Infrastructure Service		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Schematics		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Secrets Manager		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Secure Gateway		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	Server Automation		Affected	No				
IBM	Spectrum Archive Library Edition		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Spectrum Discover		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Spectrum Protect Client Management Service		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Spectrum Protect for Databases: Data Protection for Oracle		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Spectrum Protect for Databases: Data Protection for SQL		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Spectrum Protect for Enterprise Resource Planning		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Spectrum Protect for Mail: Data Protection for Domino		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Spectrum Protect for Mail: Data Protection for Exchange		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Spectrum Protect for Workstations		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Spectrum Protect for z/OS USS Client and API		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Spectrum Protect Plus Db2 Agent		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Spectrum Protect Plus Exchange Agent		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Spectrum Protect Plus File Systems Agent		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	Spectrum Protect Plus MongoDB Agent		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Spectrum Protect Plus O365 Agent		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Spectrum Protect Server		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Spectrum Protect Snapshot for UNIX		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Spectrum Protect Snapshot for UNIX		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	SQL Query		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Sterling Gentran		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Sterling Order Management		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Sterling Transformation Extender Pack for ACORD		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Sterling Transformation Extender Pack for Financial Services		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Sterling Transformation Extender Pack for FIX		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Sterling Transformation Extender Pack for NACHA		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Sterling Transformation Extender Pack for PeopleSoft		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	Sterling Transformation Extender Pack for SAP R/3		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Sterling Transformation Extender Pack for SEPA		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Sterling Transformation Extender Pack for Siebel		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Sterling Transformation Extender Pack for SWIFT		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Sterling Transformation Extender Packs for EDI		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Sterling Transformation Extender Packs for Healthcare		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Sterling Transformation Extender Trading Manager		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Storage TS1160		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Storage TS2280		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Storage TS2900 Library		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Storage TS3100-TS3200 Library		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Storage TS4500 Library		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Storage Virtualization Engine TS7700		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	Tape System Library Manager		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	TDMF for zOS		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Total Storage Service Console (TSSC) / TS4500 IMC		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Transit Gateway		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Tririga Anywhere		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	TS4300		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Urbancode Deploy		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Virtual Private Cloud		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Virtual Server for Classic		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Virtualization Management Interface		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	VMware Solutions		Affected	Yes	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	VMware vCenter Server		Affected	Yes	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	VMware vSphere		Affected	Yes	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	VPN for VPC		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	vRealize Operations and Log Insight		Affected	Yes	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Workload Automation		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
ICONICS	All		Not Affected		ICONICS Advisory Link			12/21/2021
IFS					IFS Bulletin			
IGEL					IGEL Statement			
Ignite Realtime					Ignite Realtime Statement			
iGrafx					iGrafx Statement			
Illuminated Cloud					Illuminated Cloud Statement			
Illumio	C-VEN		Not Affected		Illumio KB article			12/16/2021
Illumio	CLI		Not Affected		Illumio KB article			12/16/2021
Illumio	CloudSecure		Not Affected		Illumio KB article			12/16/2021
Illumio	Core on-premise PCE		Not Affected		Illumio KB article			12/16/2021
Illumio	Core SaaS PCE		Not Affected		Illumio KB article			12/16/2021
Illumio	Edge SaaS PCE		Not Affected		Illumio KB article			12/16/2021
Illumio	Edge-CrowdStrike		Not Affected		Illumio KB article			12/16/2021
Illumio	Flowlink		Not Affected		Illumio KB article			12/16/2021
Illumio	Kubelink		Not Affected		Illumio KB article			12/16/2021
Illumio	NEN		Not Affected		Illumio KB article			12/16/2021
Illumio	QRadar App		Not Affected		Illumio KB article			12/16/2021
Illumio	Splunk App		Not Affected		Illumio KB article			12/16/2021
Illumio	VEN		Not Affected		Illumio KB article			12/16/2021
IManage					IManage Statement			
Imperva					Imperva Statement			
Inductive Automation					Inductive Automation Statement			
IndustrialDefender					IndustrialDefender Statement			
infinidat					infinidat Statement			
InfluxData					InfluxData Statement			
Infoblox					Infoblox Statement			
Informatica					Informatica Statement			
Instana					Instana Statement			
Instructure					Instructure Statement			
Intel	Audio Development Kit		Affected	No	Intel Advisory			12/16/2021
Intel	Datacenter Manager		Affected	No	Intel Advisory			12/16/2021
Intel	oneAPI sample browser plugin for Eclipse		Affected		Intel Advisory			12/16/2021
Intel	System Debugger		Affected		Intel Advisory			12/16/2021
Intel	Secure Device Onboard		Affected		Intel Advisory			12/16/2021
Intel	Genomics Kernel Library		Affected		Intel Advisory			12/16/2021
Intel	System Studio		Affected		Intel Advisory			12/16/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Intel	Computer Vision Annotation Tool maintained by Intel		Affected		Intel Advisory			12/16/2021
Intel	Sensor Solution Firmware Development Kit		Affected		Intel Advisory			12/16/2021
Internet Systems Consortium(ISC)	ISC DHCP, aka dhcpd	All	Not Affected	N/A	ISC Open Source and Log4J	no JAVA Code		12/17/2021
Internet Systems Consortium(ISC)	Kea DHCP	All	Not Affected	N/A	ISC Open Source and Log4J	no JAVA Code		12/17/2021
Internet Systems Consortium(ISC)	BIND 9	All	Not Affected	N/A	ISC Open Source and Log4J	no JAVA Code		12/17/2021
InterSystems					InterSystems Statement			
Intland	codebeamer	<= 20.11-SP11, <= 21.09-SP3	Affected	Some releases	Apache Log4j vulnerability and fixes	A fix has been released for 20.11 and 21.09, but not yet for 21.04		
IPRO	Netgovern							
iRedMail					iRedMail Statement			
Ironnet					Ironnet Security Notification			
ISLONLINE					ISLONLINE Statement			
Ivanti					Ivanti Statement			
Jamasoftware					Jamasoftware Statement			
Jamf	Jamf Pro	10.31.0 – 10.34.0	Affected	Yes	Mitigating the Apache Log4j 2 Vulnerability			
Jaspersoft					Jaspersoft Statement			
Jedox					Jedox Statement			
Jenkins	CI/CD Core		Not Affected					
Jenkins	Plugins		Some affected, some fixed, most unaffected. See issue tracker	Some	Announcement, issue tracker	Instructions to test your installations in announcement		2021-12-16
JetBrains	IntelliJ platform based IDEs (AppCode, CLion, DataGrip, DataSpell, GoLand, IntelliJ IDEA Ultimate/Community/Edu, PhpStorm, PyCharm Professional/Community/Edu, Rider, RubyMine, WebStorm)	Unknown	Not Affected		JetBrains Blog Post			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
JetBrains	All .NET tools (ReSharper, Rider, ReSharper C++, dotTrace, dotMemory, dotCover, dotPeek)	Unknown	Not Affected		JetBrains Blog Post			
JetBrains	ToolBox	Unknown	Not Affected		JetBrains Blog Post			
JetBrains	TeamCity	Unknown	Not Affected		JetBrains Blog Post			
JetBrains	Hub	2021.1.14080	Fixed		JetBrains Blog Post			
JetBrains	YouTrack Standalone	2021.4.35970	Fixed		JetBrains Blog Post			
JetBrains	YouTrack InCloud	Unknown	Fixed		JetBrains Blog Post			
JetBrains	Datalore	Unknown	Not Affected		JetBrains Blog Post			
JetBrains	Space	Unknown	Not Affected		JetBrains Blog Post			
Jetbrains	Code With Me	Unknown	Fixed		JetBrains Blog Post			
JetBrains	Gateway	Unknown	Not Affected		JetBrains Blog Post			
JetBrains	Kotlin	Unknown	Not Affected		JetBrains Blog Post			
JetBrains	Ktor	Unknown	Not Affected		JetBrains Blog Post			
JetBrains	MPS	Unknown	Not Affected		JetBrains Blog Post			
JetBrains	Floating license server	30211	Fixed		JetBrains Blog Post			
JetBrains	UpSource	2020.1.1952	Fixed		JetBrains Blog Post			
JFROG					JFROG Statement			
Jitsi					Jitsi Advisory			
Jitterbit					Jitterbit Statement			
jPOS	(ISO-8583) bridge	Unknown	Not Affected		source			
Johnson Controls	C•CURE-9000	2.90.x (all 2.90 versions)	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	C•CURE-9000	2.80.x (all 2.80 versions)	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	C•CURE-9000	2.70 (All versions)	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	C•CURE-9000	2.60 (All versions)	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	victor	5.x	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	victor/ C•CURE-9000 Unified	3.81.x / victor 5.4.1 / C•CURE-9000 2.80	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	victor/ C•CURE-9000 Unified	3.91.x / victor 5.6.1 / C•CURE-9000 2.90	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	Metasys Products and Tools	All versions	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	Facility Explorer	14.x	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	CEM AC2000	All versions	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	CEM Hardware Products	All versions	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	Illustra Cameras	All versions	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	Illustra Insight	All versions	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	Tyco AI	All versions	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	DLS	All versions	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	Entrapass	All versions	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	CloudVue Web	All versions	Not Affected		Johnson Controls Advisory Link			12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Johnson Controls	CloudVue Gateway	All versions	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	Qolsys IQ Panels	All versions	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	PowerSeries NEO	All versions	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	PowerSeries Pro	All versions	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	Sur-Gard Receivers	All versions	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	VideoEdge	5.x	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	exacqVision Server	All versions	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	exacqVision Client	All versions	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	exacqVision WebService	All versions	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	BCPro	All versions	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	iSTAR	All versions	Not Affected		Johnson Controls Advisory Link			12/21/2021
Journyx					Journeyx Statement			
Jump Desktop					Jump Desktop Statement			
Juniper Networks					Juniper Networks Statement			
Justice Systems					Justice Systems Support			
K15t					K15t Statement			
K6					K6 Statement			
Karakun					Karakun Statement			
Kaseya					Kaseya Vulnerability Assessment			
Keeper Security					Keeper Security Notice			
KEMP					KEMP Support			
KEMP 2					KEMP 2 Support			
Kofax					Kofax Product Information			
Konica Minolta					Konica Minolta Support			
Kronos UKG					Kronos UKG Statement			
Kyberna					Kyberna Statement			
L-Soft					L-Soft Info			
L3Harris Geospatial					L3Harris Geospatial			
Lancom Systems					Lancom Systems General Security Information			
Lansweeper					Lansweeper Information			
Laserfiche					Laserfiche Product Information			
LastPass					LastPass Information			
LaunchDarkly					LaunchDarkly Statement			
Leanix					Leanix Statement			
Leica BIOSYSTEMS	Aperio AT2		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	Aperio AT2 DX		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	Aperio CS2		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	Aperio eSlide Manager		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	Aperio GT 450		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Leica BIOSYSTEMS	Aperio GT 450 DX		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	Aperio ImageScope		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	Aperio ImageScope DX		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	Aperio LV1		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	Aperio SAM DX Server For GT 450 DX		Under Investigation		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	Aperio Scanner Administration Manager (SAM) Server for GT 450		Under Investigation		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	Aperio VERSA		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	Aperio WebViewer DX		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	BOND-ADVANCE		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	BOND Controller		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	BOND-III		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	BOND-MAX		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	BOND RX		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	BOND RXm		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	CEREBRO		Under Investigation		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	CytoVision		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	HistoCore PEARL		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	HistoCore PEGASUS		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	HistoCore SPECTRA CV		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	HistoCore SPECTRA ST		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	HistoCore SPIRIT ST		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	HistoCore SPRING ST		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	Leica ASP300S		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	Leica CV5030		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	Leica ST4020		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	Leica ST5010		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	Leica ST5020		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	Leica TP1020		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	LIS Connect		Under Investigation		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	PathDX		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Leica BIOSYSTEMS	ThermoBrite Elite		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021
Lenovo	BIOS/UEFI		Not Affected		Apache Log4j Vulnerability			2021-12-14

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Lenovo	Chassis Management Module 2 (CMM)		Not Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	Commercial Vantage		Not Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	Confluent		Not Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	DSS-G		Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	Embedded System Management Java-based KVM clients		Not Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	Fan Power Controller (FPC)		Not Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	Fan Power Controller2 (FPC2)		Not Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	Integrated Management Module II (IMM2)		Not Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	NetApp ONTAP Tools for VMware vSphere		Affected		Apache Log4j Vulnerability	See NetApp advisory.		2021-12-14
Lenovo	Network Switches running: Lenovo CNOS, Lenovo ENOS, IBM ENOS, or Brocade FOS		Not Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	Storage Management utilities		Under Investigation		Apache Log4j Vulnerability			2021-12-14
Lenovo	System Management Module (SMM)		Not Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	System Management Module 2 (SMM2)		Not Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	System Update		Not Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	Thin Installer		Not Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	ThinkAgile HX		Affected		Apache Log4j Vulnerability	Nutanix and VMware components only; hardware not affected. See Nutanix and VMWare advisories.		2021-12-14

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Lenovo	ThinkAgile VX		Affected		Apache Log4j Vulnerability	VMware components only; hardware not affected. See VMWare advisory.		2021-12-14
Lenovo	ThinkSystem 2x1x16 Digital KVM Switch - Type 1754D1T		Not Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	ThinkSystem DE Series Storage		Not Affected		Apache Log4j Vulnerability	See also NetApp advisory.		2021-12-14
Lenovo	ThinkSystem DM Series Storage		Not Affected		Apache Log4j Vulnerability	See also NetApp advisory.		2021-12-14
Lenovo	ThinkSystem DS Series Storage		Not Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	ThinkSystem Manager (TSM)		Not Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	Update Retriever		Not Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	Vantage		Not Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	XClarity Administrator (LXCA)		Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	XClarity Controller (XCC)		Not Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	XClarity Energy Manager (LXEM)		Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	XClarity Essentials (LXCE)		Not Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	XClarity Integrator (LXCI) for Microsoft Azure Log Analytics		Under Investigation		Apache Log4j Vulnerability			2021-12-14
Lenovo	XClarity Integrator (LXCI) for Microsoft System Center		Not Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	XClarity Integrator (LXCI) for Nagios		Under Investigation		Apache Log4j Vulnerability			2021-12-14
Lenovo	XClarity Integrator (LXCI) for ServiceNow		Under Investigation		Apache Log4j Vulnerability			2021-12-14
Lenovo	XClarity Integrator (LXCI) for VMware vCenter		Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	XClarity Integrator (LXCI) for Windows Admin Center		Not Affected		Apache Log4j Vulnerability			2021-12-14

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Lenovo	XClarity Mobile (LXCM)		Not Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	XClarity Orchestrator (LXCO)		Not Affected		Apache Log4j Vulnerability			2021-12-14
Lenovo	XClarity Provisioning Manager (LXPM)		Not Affected		Apache Log4j Vulnerability			2021-12-14
LeoStream					LeoStream Discussion			
Let's Encrypt					Let's Enrypt Statement			
LibreNMS					LibreNMS Statement			
LifeRay					LifeRay Blog			
LifeSize					LifeSize Statement			
Lightbend					Lightbend Statement			
Lime CRM					Lime CRM Statement			
LIONGARD					LIONGARD FAQ			
LiquidFiles					LiquidFiles Statement			
LiveAction					LiveAction Statement			
Loftware					Loftware			
LOGalyze	SIEM & log analyzer tool	v4.x	Affected	No	abandoned open-source software repo (sourceforge.net)	local-log4j-vuln-scanner result: indicator for vulnerable component found in /logalyze/lib/log4j-1.2.17.jar (org/apache/log4j/net/SocketNode.class): log4j 1.2.17	Forks (github.com)	2021-12-17
LogiAnalytics					LogiAnalytics Statement			
LogicMonitor	LogicMonitor Platform		Not Affected		Log4j Security Vulnerabilities			
LogMeIn					LogMeIn Statement			
LogRhythm					LogRhythm Statement			
Looker	Looker	21.0, 21.6, 21.12, 21.16, 21.18, 21.20	Affected	Yes	Looker Statement			
LucaNet					LucaNet Statement			
Lucee					Lucee Statement			
Lyrasis	Fedora Repository	3.x,4.x,5.x,6.x	Not Affected		Fedora Repository Statement	Fedora Repository is unaffiliated with Fedora Linux. Uses logback and explicitly excludes log4j.		2021-12-14
MailStore					MailStore Statement			
Maltego					Maltego Response to Logj4			
ManageEngine	Servicedesk Plus	11305 and below	Affected		Manage Engine Advisory			12/15/2021
ManageEngine Zoho					Manage Engine Link			
ManageEngine Zoho	ADManager Plus	On-Prem			ManageEngine Vulnerability Impact			12/16/2021
ManageEngine Zoho	ADAudit Plus	On-Prem			ManageEngine Vulnerability Impact			12/16/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
ManageEngine Zoho	DataSecurity Plus	On-Prem			ManageEngine Vulnerability Impact			12/16/2021
ManageEngine Zoho	EventLog Analyzer	On-Prem			ManageEngine Vulnerability Impact			12/16/2021
ManageEngine Zoho	M365 Manager Plus	On-Prem			ManageEngine Vulnerability Impact			12/16/2021
ManageEngine Zoho	RecoveryManager Plus	On-Prem			ManageEngine Vulnerability Impact			12/16/2021
ManageEngine Zoho	Exchange Reporter Plus	On-Prem			ManageEngine Vulnerability Impact			12/16/2021
ManageEngine Zoho	Log360	On-Prem			ManageEngine Vulnerability Impact			12/16/2021
ManageEngine Zoho	Log360 UEBA	On-Prem			ManageEngine Vulnerability Impact			12/16/2021
ManageEngine Zoho	Cloud Security Plus	On-Prem			ManageEngine Vulnerability Impact			12/16/2021
ManageEngine Zoho	M365 Security Plus	On-Prem			ManageEngine Vulnerability Impact			12/16/2021
ManageEngine Zoho	Analytics Plus	On-Prem			ManageEngine Vulnerability Impact			12/16/2021
MariaDB					MariaDB Statement			
MathWorks	All MathWorks general release desktop or server products		Not Affected	No	MathWorks statement regarding CVE-2021-44228			
MathWorks Matlab					MathWorks Matlab Statement			
Matillion					Matillion Security Advisory			
Matomo					Matomo Statement			
Mattermost FocalBoard					Mattermost FocalBoard Concern			
McAfee	Data Exchange Layer (DXL) Client		Not Affected					12/20/2021
McAfee	Data Loss Prevention (DLP) Discover		Not Affected					12/20/2021
McAfee	Data Loss Prevention (DLP) Endpoint for Mac		Not Affected					12/20/2021
McAfee	Data Loss Prevention (DLP) Endpoint for Windows		Not Affected					12/20/2021
McAfee	Data Loss Prevention (DLP) Monitor		Not Affected					12/20/2021
McAfee	Data Loss Prevention (DLP) Prevent		Not Affected					12/20/2021
McAfee	Endpoint Security (ENS) for Linux		Not Affected					12/20/2021
McAfee	Endpoint Security (ENS) for Mac		Not Affected					12/20/2021
McAfee	Endpoint Security (ENS) for Windows		Not Affected					12/20/2021
McAfee	ePolicy Orchestrator Application Server (ePO)	5.10 CU11	Fixed	Yes	https://kc.mcafee.com/agent/index?page=content&id=SB10377			12/20/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
McAfee	ePolicy Orchestrator Agent Handlers (ePO-AH)		Not Affected					12/20/2021
McAfee	Host Intrusion Prevention (Host IPS)		Not Affected					12/20/2021
McAfee	Management of Native Encryption (MNE)		Not Affected					12/20/2021
McAfee	McAfee Active Response (MAR)		Not Affected					12/20/2021
McAfee	McAfee Agent (MA)		Not Affected					12/20/2021
McAfee	McAfee Application and Change Control (MACC) for Linux		Not Affected					12/20/2021
McAfee	McAfee Application and Change Control (MACC) for Windows		Not Affected					12/20/2021
McAfee	McAfee Client Proxy (MCP) for Mac		Not Affected					12/20/2021
McAfee	McAfee Client Proxy (MCP) for Windows		Not Affected					12/20/2021
McAfee	McAfee Drive Encryption (MDE)		Not Affected					12/20/2021
McAfee	McAfee Security for Microsoft Exchange (MSME)		Not Affected					12/20/2021
McAfee	McAfee Security for Microsoft SharePoint (MSMS)		Not Affected					12/20/2021
McAfee	McAfee Security for Microsoft Exchange (MSME)		Not Affected					12/20/2021
McAfee	Enterprise Security Manager (ESM)	11.5.3	Fixed	Yes	https://kc.mcafee.com/agent/index?page=content&id=SB10377			12/20/2021
McAfee	Network Security Manager (NSM)		Not Affected					12/20/2021
McAfee	Network Security Platform (NSP)		Not Affected					12/20/2021
McAfee	Policy Auditor		Not Affected					12/20/2021
McAfee	Threat Intelligence Exchange (TIE)		Affected		https://kc.mcafee.com/agent/index?page=content&id=SB10377	Latest status in linked Security Bulletin		12/20/2021
McAfee	Web Gateway (MWG)		Foxed		https://kc.mcafee.com/agent/index?page=content&id=SB10377			12/20/2021
Medtronic			Under Investigation		Medtronic Advisory Link			12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
MEINBERG					MEINBERG Information			
Meltano	Meltano		Not affected		Meltano	Project is written in Python		
Memurai					Memurai Information			
MicroFocus					MicroFocus Statement			
Microsoft	Azure Application Gateway		Not Affected		Microsoft's Response to CVE-2021-44228 Apache Log4j 2			
Microsoft	Azure API Gateway		Not Affected		Microsoft's Response to CVE-2021-44228 Apache Log4j 2			
Microsoft	Azure Data lake store java	< 2.3.10	Affected		azure-data-lake-store-java/CHANGES.md at ed5d6304783286c3cfff0a1dee457a922e23ad48 · Azure/azure-data-lake-store-java · GitHub			
Microsoft	Azure Data lake store java	< 2.3.10	Affected		azure-data-lake-store-java/CHANGES.md at ed5d6304783286c3cfff0a1dee457a922e23ad48 · Azure/azure-data-lake-store-java · GitHub			
Microsoft	Azure DevOps Server	2019.0 - 2020.1	Affected	No	Azure DevOps (and Azure DevOps Server) and the log4j vulnerability			
Microsoft	Azure DevOps		Not Affected		Azure DevOps (and Azure DevOps Server) and the log4j vulnerability			
Microsoft	Azure Traffic Manager		Not Affected		Microsoft's Response to CVE-2021-44228 Apache Log4j 2			
Microsoft	Team Foundation Server	2018.2+	Affected	No	Azure DevOps (and Azure DevOps Server) and the log4j vulnerability			
Microstrategy					Microstrategy Statement			
Midori Global					Midori Global Statement			
Mikrotik					Mikrotik Statement			
Milestone sys					Milestone sys Statement			
Mimecast					Mimecast Information			
Minecraft					Minecraft Vulnerability Message			
Mirantis					Mirantis Statement			
Miro					Miro Log4j Updates			
Mitel					Mitel Statement			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
MobileIron	Core	All Versions	Affected	Yes	https://forums.ivanti.com/s/article/Security-Bulletin-CVE-2021-44228-Remote-code-injection-in-Log4j?language=en_US	The mitigation instructions listed in a subsequent section removes a vulnerable Java class (JNDILookUp.class) from the affected Log4J Java library and as a result removes the ability to perform the RCE attack. The workaround needs to be applied in a maintenance window. You will not be able to access the admin portal during the procedure, however, end user devices will continue to function.		12/20/21

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
MobileIron	Core Connector	All Versions	Affected	Yes	https://forums.ivanti.com/s/article/Security-Bulletin-CVE-2021-44228-Remote-code-injection-in-Log4j?language=en_US	The mitigation instructions listed in a subsequent section removes a vulnerable Java class (JNDILookUp.class) from the affected Log4J Java library and as a result removes the ability to perform the RCE attack. The workaround needs to be applied in a maintenance window. You will not be able to access the admin portal during the procedure, however, end user devices will continue to function.		12/20/21

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
MobileIron	Reporting Database (RDB)	All Versions	Affected	Yes	https://forums.ivanti.com/s/article/Security-Bulletin-CVE-2021-44228-Remote-code-injection-in-Log4j?language=en_US	The mitigation instructions listed in a subsequent section removes a vulnerable Java class (JNDILookUp.class) from the affected Log4J Java library and as a result removes the ability to perform the RCE attack. The workaround needs to be applied in a maintenance window. You will not be able to access the admin portal during the procedure, however, end user devices will continue to function.		12/20/21

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
MobileIron	Sentry	9.13, 9.14	Affected	Yes	https://forums.ivanti.com/s/article/Security-Bulletin-CVE-2021-44228-Remote-code-injection-in-Log4j?language=en_US	The mitigation instructions listed in a subsequent section removes a vulnerable Java class (JNDILookUp.class) from the affected Log4J Java library and as a result removes the ability to perform the RCE attack. The workaround needs to be applied in a maintenance window. You will not be able to access the admin portal during the procedure, however, end user devices will continue to function.		12/20/21
MongoDB	All other components of MongoDB Atlas (including Atlas Database, Data Lake, Charts)		Not Affected		https://www.mongodb.com/blog/post/log4shell-vulnerability-cve-2021-44228-and-mongodb			
MongoDB	MongoDB Atlas Search		Affected	yes	https://www.mongodb.com/blog/post/log4shell-vulnerability-cve-2021-44228-and-mongodb			
MongoDB	MongoDB Community Edition (including Community Server, Cloud Manager, Community Kubernetes Operators)		Not Affected		https://www.mongodb.com/blog/post/log4shell-vulnerability-cve-2021-44228-and-mongodb			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
MongoDB	MongoDB Drivers		Not Affected		https://www.mongodb.com/blog/post/log4shell-vulnerability-cve-2021-44228-and-mongodb			
MongoDB	MongoDB Enterprise Advanced (including Enterprise Server, Ops Manager, Enterprise Kubernetes Operators)		Not Affected		https://www.mongodb.com/blog/post/log4shell-vulnerability-cve-2021-44228-and-mongodb			
MongoDB	MongoDB Realm (including Realm Database, Sync, Functions, APIs)		Not Affected		https://www.mongodb.com/blog/post/log4shell-vulnerability-cve-2021-44228-and-mongodb			
MongoDB	MongoDB Tools (including Compass, Database Shell, VS Code Plugin, Atlas CLI, Database Connectors)		Not Affected		https://www.mongodb.com/blog/post/log4shell-vulnerability-cve-2021-44228-and-mongodb			
Moodle					Moodle Discussion			
MoogSoft					MoogSoft Vulnerability Information			
Motorola Avigilon					Motorola Avigilon Technical Notification			
Mulesoft					Mulesoft Statement	This advisory is available to customers only and has not been reviewed by CISA		
Mulesoft	Mule Runtime	3.x,4.x	Affected	Yes	Apache Log4j2 vulnerability - December 2021	This advisory is available to account holders only and has not been reviewed by CISA.		12/15/2021
Mulesoft	Mule Agent	6.x	Affected	Yes	Apache Log4j2 vulnerability - December 2021	This advisory is available to account holders only and has not been reviewed by CISA.		12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Mulesoft	Cloudhub		Affected	Yes	Apache Log4j2 vulnerability - December 2021	This advisory is available to account holders only and has not been reviewed by CISA.		12/15/2021
Mulesoft	Anypoint Studio	7.x	Affected	Yes	Apache Log4j2 vulnerability - December 2021	This advisory is available to account holders only and has not been reviewed by CISA.		12/15/2021
N-able					N-able Statement			
Nagios					Nagios Statement			
NAKIVO					NAKIVO Statement			
Neo4j	Neo4j Graph Database	Version >4.2, <4..2.12	Affected	No				12/13/2021
Netapp	Multiple NetApp products		Affected		https://security.netapp.com/advisory/ntap-20211210-0007/			
Netcup					Netcup Statement			
NetGate PFSense					NetGate PFSense Forum			
Netwrix					Netwrix Statement			
New Relic	Containerized Private Minion (CPM)	3.0.57	Fixed	Yes	NR21-04	New Relic is in the process of revising guidance/documentation, however the fix version remains sufficient.	Security Bulletin NR21-04	12-18-2021
New Relic	New Relic Java Agent	<7.4.3	Affected	Yes	https://docs.newrelic.com/docs/release-notes/agent-release-notes/java-release-notes/java-agent-743/	Initially fixed in 7.4.2, but additional vulnerability found	New Relic tracking, covers CVE-2021-44228, CVE-2021-45046	12/20/2021
NextCloud					NextCloud Help			
Nextflow	Nextflow	21.04.0.5552	Not Affected		https://www.nextflow.io/docs/latest/index.html			12/21/2021
Nexus Group					Nexus Group Docs			
NI (National Instruments)					NI Support Link			
Nice Software (AWS) EnginFRAME					Nice Software EnginFRAME Link			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
NinjaRMM					NinjaRMM Article	This advisory is available to customers only and has not been reviewed by CISA		
Nomachine					Nomachine Forums			
NoviFlow					Noviflow Link			
Nulab	Backlog	N/A (SaaS)	Fixed		Nulab Blog Post			
Nulab	Backlog Enterprise (On-premises)	< 1.11.7	Fixed	Yes	Nulab Blog Post			
Nulab	Cacoo	N/A (SaaS)	Fixed		Nulab Blog Post			
Nulab	Cacoo Enterprise (On-premises)	< 4.0.4	Fixed	Yes	Nulab Blog Post			
Nulab	Typetalk	N/A (SaaS)	Fixed		Nulab Blog Post			
Nutanix	AHV	All	Not Affected		Nutanix Security Advisory			12/20/2021
Nutanix	AOS	LTS (including Prism Element), Community Edition	Not Affected		Nutanix Security Advisory			12/20/2021
Nutanix	AOS	STS (including Prism Element)	Fixed	Yes	Nutanix Security Advisory	Patched in 6.0.2.4, available on the Portal for		
download		12/20/2021						
Nutanix	Beam		Fixed		Nutanix Security Advisory	Saas-Based Procuct. See Advisory.		12/20/2021
Nutanix	BeamGov		Fixed		Nutanix Security Advisory	Saas-Based Procuct. See Advisory.		12/20/2021
Nutanix	Calm	All	Not Affected		Nutanix Security Advisory			12/20/2021
Nutanix	Calm Tunnel VM	All	Not Affected		Nutanix Security Advisory			12/20/2021
Nutanix	Collector	All	Not Affected		Nutanix Security Advisory			12/20/2021
Nutanix	Collector Portal		Fixed		Nutanix Security Advisory	Saas-Based Procuct. See Advisory.		12/20/2021
Nutanix	Data Lens		Not Affected		Nutanix Security Advisory	Saas-Based Procuct. See Advisory.		12/20/2021
Nutanix	Era	All	Not Affected		Nutanix Security Advisory			12/20/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Nutanix	File Analytics	2.1.x, 2.2.x, 3.0+	Affected		Nutanix Security Advisory	Mitigated in version 3.0.1 which is available on the Portal for download. Mitigation is available here		12/20/2021
Nutanix	Files	All	Not Affected		Nutanix Security Advisory			12/20/2021
Nutanix	Flow	All	Not Affected		Nutanix Security Advisory			12/20/2021
Nutanix	Flow Security Cental		Fixed		Nutanix Security Advisory	Saas-Based Procuct. See Advisory.		12/20/2021
Nutanix	Foundation	All	Not Affected		Nutanix Security Advisory			12/20/2021
Nutanix	Frame		Fixed		Nutanix Security Advisory	Saas-Based Procuct. See Advisory.		12/20/2021
Nutanix	FrameGov		Fixed		Nutanix Security Advisory	Saas-Based Procuct. See Advisory.		12/20/2021
Nutanix	FSCVM	All	Not Affected		Nutanix Security Advisory			12/20/2021
Nutanix	Insights		Not Affected		Nutanix Security Advisory	Saas-Based Procuct. See Advisory.		12/20/2021
Nutanix	Karbon	All	Affected		Nutanix Security Advisory	Mitigation is available here		12/20/2021
Nutanix	Karbon Platform Service		Fixed		Nutanix Security Advisory	Saas-Based Procuct. See Advisory.		12/20/2021
Nutanix	Leap		Fixed		Nutanix Security Advisory	Saas-Based Procuct. See Advisory.		12/20/2021
Nutanix	LCM	All	Not Affected		Nutanix Security Advisory			12/20/2021
Nutanix	Mine	All	Affected		Nutanix Security Advisory	Mitigation is available here		12/20/2021
Nutanix	Move	All	Not Affected		Nutanix Security Advisory			12/20/2021
Nutanix	MSP	All	Affected		Nutanix Security Advisory	Mitigation is available here		12/20/2021
Nutanix	NCC	All	Not Affected		Nutanix Security Advisory			12/20/2021
Nutanix	NGT	All	Not Affected		Nutanix Security Advisory			12/20/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Nutanix	Objects	All	Affected		Nutanix Security Advisory	Mitigation is available here		12/20/2021
Nutanix	Prism Central	All	Fixed		Nutanix Security Advisory	Patched in 2021-9.0.3, available on the Portal for download.		12/20/2021
Nutanix	Sizer		Fixed		Nutanix Security Advisory	Saas-Based Procuct. See Advisory.		12/20/2021
Nutanix	Volumes	All	Not Affected		Nutanix Security Advisory			12/20/2021
Nutanix	Witness VM	All	Affected		Nutanix Security Advisory	Mitigation is available here		12/20/2021
Nutanix	X-Ray	All	Not Affected		Nutanix Security Advisory			12/20/2021
Nvidia					Nvidia Link			
NXLog					NXLog Link			
Objectif Lune					Objectif Lune Blog Post			
OCLC					OCLC Link			
Octopus					Octopus Advisory			
Okta	Advanced Server Access		Not Affected		Okta's response to CVE-2021-44228 ("Log4Shell") Okta Security			12/12/2021
Okta	Okta Access Gateway		Not Affected		Okta's response to CVE-2021-44228 ("Log4Shell") Okta Security			12/12/2021
Okta	Okta AD Agent		Not Affected		Okta's response to CVE-2021-44228 ("Log4Shell") Okta Security			12/12/2021
Okta	Okta Browser Plugin		Not Affected		Okta's response to CVE-2021-44228 ("Log4Shell") Okta Security			12/12/2021
Okta	Okta IWA Web Agent		Not Affected		Okta's response to CVE-2021-44228 ("Log4Shell") Okta Security			12/12/2021
Okta	Okta LDAP Agent		Not Affected		Okta's response to CVE-2021-44228 ("Log4Shell") Okta Security			12/12/2021
Okta	Okta Mobile		Not Affected		Okta's response to CVE-2021-44228 ("Log4Shell") Okta Security			12/12/2021
Okta	Okta RADIUS Server Agent	< 2.17.0	Affected		Okta RADIUS Server Agent CVE-2021-44228 Okta			12/12/2021
Okta	Okta Verify		Not Affected		Okta's response to CVE-2021-44228 ("Log4Shell") Okta Security			12/12/2021
Okta	Okta Workflows		Not Affected		Okta's response to CVE-2021-44228 ("Log4Shell") Okta Security			12/12/2021
Okta	Okta On-Prem MFA Agent	< 1.4.6	Affected		Okta On-Prem MFA Agent CVE-2021-44228 Okta			12/12/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Onespan					Onespan Link			
Opengear					Opengear Link			
OpenMRS TALK					OpenMRS TALK Link			
OpenNMS					OpenNMS Link			
OpenSearch					OpenSearch Discussion Link			
Oracle			Affected		Oracle Security Alert My Oracle Support Document	The support document is available to customers only and has not been reviewed by CISA		12/17/2021
Orgavision					Orgavision Link			
Osirium	PAM		Not Affected		Osirium statement			
Osirium	PEM		Not Affected		Osirium statement			
Osirium	PPA		Not Affected		Osirium statement			
OTRS					OTRS Link			
OVHCloud					OVHCloud Blog Post			
OwnCloud					OwnCloud Link			
OxygenXML	Author		Affected	Fixed	Yes	https://www.oxygenxml.com/security/advisory/CVE-2021-44228.html		12/17/2021
OxygenXML	Developer		Affected	Fixed	Yes	https://www.oxygenxml.com/security/advisory/CVE-2021-44228.html		12/17/2021
OxygenXML	Editor		Affected	Fixed	Yes	https://www.oxygenxml.com/security/advisory/CVE-2021-44228.html		12/17/2021
OxygenXML	Oxygen Content Fusion	2.0, 3.0, 4.1	Affected	Fixed	Yes	https://www.oxygenxml.com/security/advisory/CVE-2021-44228.html		12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
OxygenXML	Oxygen Feedback Enterprise	1.4.4 & older	Affected	Fixed	Yes	https://www.oxygenxml.com/security/advisory/CVE-2021-44228.html		12/17/2021
OxygenXML	Oxygen License Server	v22.1 to v24.0	Affected	Fixed	Yes	https://www.oxygenxml.com/security/advisory/CVE-2021-44228.html		12/17/2021
OxygenXML	Oxygen PDF Chemistry	v22.1, 23.0, 23.1, 24.0	Affected	Fixed	Yes	https://www.oxygenxml.com/security/advisory/CVE-2021-44228.html		12/17/2021
OxygenXML	Oxygen SDK		Affected	Fixed	Yes	https://www.oxygenxml.com/security/advisory/CVE-2021-44228.html		12/17/2021
OxygenXML	Plugins (see advisory link)		Affected	Fixed	Yes	https://www.oxygenxml.com/security/advisory/CVE-2021-44228.html		12/17/2021
OxygenXML	Publishing Engine		Affected	Fixed	Yes	https://www.oxygenxml.com/security/advisory/CVE-2021-44228.html		12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
OxygenXML	Web Author		Affected	Fixed	Yes	https://www.oxygenxml.com/security/advisory/CVE-2021-44228.html		12/17/2021
OxygenXML	WebHelp		Affected	Fixed	Yes	https://www.oxygenxml.com/security/advisory/CVE-2021-44228.html		12/17/2021
Palantir	Palantir Foundry	All	Fixed		Palantir Response to Log4j Vulnerability (palantir.com)	No impact to Palantir-hosted or Apollo-connected instances, and updates have been deployed for full remediation. Disconnected customer instances may require manual updates.		12/19/2021
Palantir	Palantir Gotham	All	Fixed		Palantir Response to Log4j Vulnerability (palantir.com)	No impact to Palantir-hosted or Apollo-connected instances, and updates have been deployed for full remediation. Disconnected customer instances may require manual updates.		12/19/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Palantir	Palantir Apollo	All	Not Affected		Palantir Response to Log4j Vulnerability (palantir.com)	No impact, and updates have been deployed for full remediation.		12/19/2021
Palantir	Palantir AI Inference Platform (AIP)	All	Fixed		Palantir Response to Log4j Vulnerability (palantir.com)	Fully remediated as of 1.97.0. Disconnected customer instances may require manual updates.		12/19/2021
Palo-Alto Networks	CloudGenix		Not Affected		CVE-2021-44228 Informational: Impact of Log4j Vulnerability CVE-2021-44228 (paloaltonetworks.com)			
Palo-Alto Networks	Palo-Alto Networks-OS for Panorama	9.0, 9.1, 10.0	Affected	Yes	CVE-2021-44228:Impact of Log4J Vulnerability		Upgrade Panorama to PAN-OS 10.1 to remediate this issue. This advisory will be updated when hot fixes for the affected Panorama versions are available. PAN-OS for Panorama versions 8.1, 10.1 are not affected.	12/15/2021
Palo-Alto Networks	Bridgecrew		Not Affected		CVE-2021-44228 Informational: Impact of Log4j Vulnerability CVE-2021-44228 (paloaltonetworks.com)			
Palo-Alto Networks	Cortex Data Lake		Not Affected		CVE-2021-44228 Informational: Impact of Log4j Vulnerability CVE-2021-44228 (paloaltonetworks.com)			
Palo-Alto Networks	Cortex Xpanse		Not Affected		CVE-2021-44228 Informational: Impact of Log4j Vulnerability CVE-2021-44228 (paloaltonetworks.com)			
Palo-Alto Networks	Cortex XDR Agent		Not Affected		CVE-2021-44228 Informational: Impact of Log4j Vulnerability CVE-2021-44228 (paloaltonetworks.com)			
Palo-Alto Networks	Cortex XSOAR		Not Affected		CVE-2021-44228 Informational: Impact of Log4j Vulnerability CVE-2021-44228 (paloaltonetworks.com)			
Palo-Alto Networks	Expedition		Not Affected		CVE-2021-44228 Informational: Impact of Log4j Vulnerability CVE-2021-44228 (paloaltonetworks.com)			
Palo-Alto Networks	IoT Security		Not Affected		CVE-2021-44228 Informational: Impact of Log4j Vulnerability CVE-2021-44228 (paloaltonetworks.com)			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Palo-Alto Networks	GlobalProtect App		Not Affected		CVE-2021-44228 Informational: Impact of Log4j Vulnerability CVE-2021-44228 (paloaltonetworks.com)			
Palo-Alto Networks	Palo-Alto Networks-OS for Firewall and Wildfire		Not Affected		CVE-2021-44228 Informational: Impact of Log4j Vulnerability CVE-2021-44228 (paloaltonetworks.com)			
Palo-Alto Networks	Prisma Access		Not Affected		CVE-2021-44228 Informational: Impact of Log4j Vulnerability CVE-2021-44228 (paloaltonetworks.com)			
Palo-Alto Networks	Prisma Cloud		Not Affected		CVE-2021-44228 Informational: Impact of Log4j Vulnerability CVE-2021-44228 (paloaltonetworks.com)			
Palo-Alto Networks	Prisma Cloud Compute		Not Affected		CVE-2021-44228 Informational: Impact of Log4j Vulnerability CVE-2021-44228 (paloaltonetworks.com)			
Palo-Alto Networks	Okyo Grade		Not Affected		CVE-2021-44228 Informational: Impact of Log4j Vulnerability CVE-2021-44228 (paloaltonetworks.com)			
Palo-Alto Networks	SaaS Security		Not Affected		CVE-2021-44228 Informational: Impact of Log4j Vulnerability CVE-2021-44228 (paloaltonetworks.com)			
Palo-Alto Networks	WildFire Appliance		Not Affected		CVE-2021-44228 Informational: Impact of Log4j Vulnerability CVE-2021-44228 (paloaltonetworks.com)			
Palo-Alto Networks	WildFire Cloud		Not Affected		CVE-2021-44228 Informational: Impact of Log4j Vulnerability CVE-2021-44228 (paloaltonetworks.com)			
Palo-Alto Networks	User-ID Agent		Not Affected		CVE-2021-44228 Informational: Impact of Log4j Vulnerability CVE-2021-44228 (paloaltonetworks.com)			
Panopto					Panopto Support Link			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
PaperCut	PaperCut MF	21.0 and later	Affected	Yes	https://www.papercut.com/support/known-issues/?id=PO-684#ng	Versions 21.0 and later are impacted. Versions 20 and earlier are NOT impacted by this. Workaround manual steps available in reference. Upgrade to PaperCut NG/MF version 21.2.3 Now Available to resolve.		12/16/2021
PaperCut	PaperCut NG	21.0 and later	Affected	Yes	https://www.papercut.com/support/known-issues/?id=PO-684#ng	Versions 21.0 and later are impacted. Versions 20 and earlier are NOT impacted by this. Workaround manual steps available in reference. Upgrade to PaperCut NG/MF version 21.2.3 Now Available to resolve.		12/16/2021
Parallels					Parellels Link			
Parse.ly					Parse.ly Blog Post			
PBXMonitor	RMM for 3CX PBX		Not Affected		PBXMonitor Changelog	Mirror Servers were also checked to ensure Log4J was not installed or being used by any of our systems.		12/22/2021
Pega					Pega Docs Link			
Pentaho					Pentaho Support Link			
Pepperl+Fuchs			Under Investigation		Pepperl+Fuchs Advisory Link			12/21/2021
Percona					Percona Blog Post			
Pexip					Pexip Link			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Phenix Id					Phenix Id Support Link			
Philips	Multiple products				Philips Security Advisory			
PHOENIX CONTACT	Physical products containing firmware		Not Affected		PHOENIX CONTACT Advisory Link			12/22/2021
PHOENIX CONTACT	Software Products		Not Affected		PHOENIX CONTACT Advisory Link			12/22/2021
PHOENIX CONTACT	Cloud Services		Affected		PHOENIX CONTACT Advisory Link	Partly affected. Remediations are being implemented.		12/22/2021
Ping Identity	PingAccess	4.0 <= version <= 6.3.2	Affected	Yes	Log4j2 vulnerability CVE-2021-44228			2021-12-15
Ping Identity	PingCentral		Affected	Yes	Log4j2 vulnerability CVE-2021-44228			2021-12-15
Ping Identity	PingFederate	8.0 <= version <= 10.3.4	Affected	Yes	Log4j2 vulnerability CVE-2021-44228			2021-12-15
Ping Identity	PingFederate Java Integration Kit	< 2.7.2	Affected	Yes	Log4j2 vulnerability CVE-2021-44228			2021-12-15
Ping Identity	PingFederate OAuth Playground	< 4.3.1	Affected	Yes	Log4j2 vulnerability CVE-2021-44228			2021-12-15
Ping Identity	PingIntelligence		Affected	Yes	Log4j2 vulnerability CVE-2021-44228			2021-12-15
Pitney Bowes					Pitney Bowes Support Link			
Planmeca					Planmeca Link			
Planon Software					Planon News	This advisory is available for customers only and has not been reviewed by CISA		
Platform.SH					Platform.SH Blog Post			
Plesk					Plesk Support Link			
Plex	Plex Industrial IoT		Fixed		PN1579 - Log4Shell Vulnerability Notice	The product has been updated to Log4j version 2.15. An additional patch is being developed to update to 2.16. No user interaction is required.		12/15/2021
Polycom					Polycom Support Link			
Portainer					Portainer Blog Post			
PortSwigger					PortSwigger Forum			
PostGreSQL					PostGreSQL News			
Postman					Postman Support Link			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Power Admin LLC	PA File Sight	NONE	Not Affected		Update December 2021: None of our products (PA Server Monitor, PA Storage Monitor, PA File Sight and PA WatchDISK), and none of our websites, use log4j. One less thing to worry about			12/17/2021
Power Admin LLC	PA Storage Monitor	NONE	Not Affected		Update December 2021: None of our products (PA Server Monitor, PA Storage Monitor, PA File Sight and PA WatchDISK), and none of our websites, use log4j. One less thing to worry about			12/17/2021
Power Admin LLC	PA Server Monitor	NONE	Not Affected		Update December 2021: None of our products (PA Server Monitor, PA Storage Monitor, PA File Sight and PA WatchDISK), and none of our websites, use log4j. One less thing to worry about			12/17/2021
Pretix					Pretix Blog Post			
PrimeKey					PrimeKey Support Link			
Progress / IpSwitch					Progress / IpSwitch Link			
ProofPoint					ProofPoint Article	This advisory is available for customers only and has not been reviewed by CISA		
ProSeS					ProSeS Link			
Prosys					Prosys News Link			
Proxmox					Proxmox Forum			
PRTG Paessler					PRTG Paessler Link			
PTC	Axeda Platform	6.9.2	Affected	No	PTC Axeda Platform Apache log4j vulnerability - Incident Response			12/17/2021
PTC	ThingsWorx Platform	8.5,9.0,9.1,9.2, All supported versions	Affected	No	ThingWorx Apache log4j vulnerability - Incident Response			12/17/2021
PTC	ThingsWorx Analytics	8.5,9.0,9.1,9.2, All supported versions	Affected	No	ThingWorx Apache log4j vulnerability - Incident Response			12/17/2021
PTV Group					PTV Group Link			
Pulse Secure	Ivanti Connect Secure (ICS)		Not Affected		Pulse Secure Article: KB44933 - CVE-2021-44228 - Java logging library (log4j)			
Pulse Secure	Ivanti Neurons for secure Access		Not Affected		Pulse Secure Article: KB44933 - CVE-2021-44228 - Java logging library (log4j)			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Pulse Secure	Ivanti Neurons for ZTA		Not Affected		Pulse Secure Article: KB44933 - CVE-2021-44228 - Java logging library (log4j)			
Pulse Secure	Pulse Connect Secure		Not Affected		Pulse Secure Article: KB44933 - CVE-2021-44228 - Java logging library (log4j)			
Pulse Secure	Pulse Desktop Client		Not Affected		Pulse Secure Article: KB44933 - CVE-2021-44228 - Java logging library (log4j)			
Pulse Secure	Pulse Mobile Client		Not Affected		Pulse Secure Article: KB44933 - CVE-2021-44228 - Java logging library (log4j)			
Pulse Secure	Pulse One		Not Affected		Pulse Secure Article: KB44933 - CVE-2021-44228 - Java logging library (log4j)			
Pulse Secure	Pulse Policy Secure		Not Affected		Pulse Secure Article: KB44933 - CVE-2021-44228 - Java logging library (log4j)			
Pulse Secure	Pulse Secure Services Director		Not Affected		Pulse Secure Article: KB44933 - CVE-2021-44228 - Java logging library (log4j)			
Pulse Secure	Pulse Secure Virtual Traffic Manager		Not Affected		Pulse Secure Article: KB44933 - CVE-2021-44228 - Java logging library (log4j)			
Pulse Secure	Pulse Secure Web Application Firewall		Not Affected		Pulse Secure Article: KB44933 - CVE-2021-44228 - Java logging library (log4j)			
Pulse Secure	Pulse ZTA		Not Affected		Pulse Secure Article: KB44933 - CVE-2021-44228 - Java logging library (log4j)			
Puppet					Puppet Blog Post			
Pure Storage					Pure Storage Support Link	This advisory is available for customers only and has not been reviewed by CISA		
Pulse Secure	Ivanti Neurons for ZTA		Not Affected		Pulse Secure Article: KB44933 - CVE-2021-44228 - Java logging library (log4j)			
Pulse Secure	Ivanti Neurons for secure Access		Not Affected		Pulse Secure Article: KB44933 - CVE-2021-44228 - Java logging library (log4j)			
Pure Storage	FlashBlade	3.1.x,3.2.x,3.3.x	Affected	No	Pure Storage Customer Portal	Patch expected 12/24/2021		12/15/2021
Pure Storage	Flash Array	5.3.x, 6.0.x, 6.1.x, 6.2.x	Affected	No	Pure Storage Customer Portal	Patch expected 12/20/2021		12/15/2021
Pure Storage	Cloud Blockstore	CBS6.1.x, CBS6.2.x	Affected	No	Pure Storage Customer Portal	Patch expected 12/27/2021		12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Pure Storage	Pure1	N/A	Fixed	Yes	Pure Storage Customer Portal			12/15/2021
Pure Storage	PortWorx	2.8.0+	Affected	Yes	Pure Storage Customer Portal			12/15/2021
Pyramid Analytics					Pyramid Analytics Community Link			
QF-Test					QF-Test Blog Post			
Qlik					Qlik Community Link			
QMATIC	Orchestra Central	6.0+	Not Affected		QMATIC Link			12/21/2021
QMATIC	Appointment Booking	2.4+	Affected	Yes	QMATIC Link	Update to v. 2.8.2 which contains log4j 2.16		12/21/2021
QMATIC	Insights	Cloud	Affected	Yes	QMATIC Link	log4j 2.16 applied 2021-12-16		12/21/2021
QMATIC	Appointment Booking	Cloud/Managed Service	Affected	Yes	QMATIC Link	log4j 2.16 applied 2021-12-15		12/21/2021
QNAP			Under Investigation		QNAP Security Advisory			
QOPPA					QOPPA Link			
QSC Q-SYS					QSC Q-SYS Article			
QT			Not Affected		QT			
Quest Global					Quest Global			
R	R	4.1.1	Not Affected		https://www.r-project.org/			12/21/2021
R2ediviewer					R2ediviewer Link			
Radware					Radware Support Link			
Rapid7	AlcidekArt, kAdvisor, and kAudit	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	AppSpider Enterprise	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	AppSpider Pro	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	Insight Agent	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	InsightAppSec Scan Engine	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	InsightAppSec Scan Engine	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	InsightCloudSec/DivvyCloud	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	InsightConnect Orchestrator	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	InsightIDR Network Sensor	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	InsightIDR/InsightOps Collector & Event Sources	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	InsightOps DataHub	InsightOps DataHub <= 2.0	Affected	Yes	Rapid7 Statement	Upgrade DataHub to version 2.0.1 using the following instructions.		12/15/2021
Rapid7	InsightOps non-Java logging libraries	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	InsightOps r7insight_java logging library	<=3.0.8	Affected	Yes	Rapid7 Statement	Upgrade r7insight_java to 3.0.9		12/15/2021
Rapid7	InsightVM Kubernetes Monitor	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	InsightVM/Nexpose	on-prem	Not Affected		Rapid7 Statement			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Rapid7	InsightVM/Nexpose Console	on-prem	Not Affected		Rapid7 Statement	Installations of the InsightVM/Nexpose have “log4j-over-slf4j-1.7.7.jar” packaged in them. This is a different library than log4j-core and is not vulnerable to Log4Shell.		12/15/2021
Rapid7	InsightVM/Nexpose Engine	on-prem	Not Affected		Rapid7 Statement	Installations of the InsightVM/Nexpose have “log4j-over-slf4j-1.7.7.jar” packaged in them. This is a different library than log4j-core and is not vulnerable to Log4Shell.		12/15/2021
Rapid7	IntSights virtual appliance	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	Logentries DataHub	Linux version <= 1.2.0.820; Windows version <= 1.2.0.820	Affected	Yes	Rapid7 Statement	Linux: Install DataHub_1.2.0.822.deb using the following instructions. Windows: Run version 1.2.0.822 in a Docker container or as a Java command per these instructions. You can find more details here.		12/15/2021
Rapid7	Logentries le_java logging library	All versions: this is a deprecated component	Affected	Yes	Rapid7 Statement	Migrate to version 3.0.9 of r7insight_java		12/15/2021
Rapid7	Metasploit Framework	on-prem	Not Affected		Rapid7 Statement			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Rapid7	Metasploit Pro	on-prem	Not Affected		Rapid7 Statement	Metasploit Pro ships with log4j but has specific configurations applied to it that mitigate Log4Shell. A future update will contain a fully patched version of log4j.		12/15/2021
Rapid7	tCell Java Agent	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	Velociraptor	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Raritan					Raritan Support Link			
Ravelin					Ravelin Link			
Real-Time Innovations (RTI)	Distributed Logger		Not Affected		RTI Statement			12/16/2021
Real-Time Innovations (RTI)	Recording Console		Not Affected		RTI Statement			12/16/2021
Real-Time Innovations (RTI)	RTI Administration Console		Not Affected		RTI Statement			12/16/2021
Real-Time Innovations (RTI)	RTI Code Generator		Not Affected		RTI Statement			12/16/2021
Real-Time Innovations (RTI)	RTI Code Generator Server		Not Affected		RTI Statement			12/16/2021
Real-Time Innovations (RTI)	RTI Micro Application Generator (MAG)	as part of RTI Connext Micro 3.0.0, 3.0.1, 3.0.2, 3.0.3	Affected		RTI Statement			12/16/2021
Real-Time Innovations (RTI)	RTI Micro Application Generator (MAG)	as part of RTI Connext Professional 6.0.0 and 6.0.1	Affected		RTI Statement			12/16/2021
Real-Time Innovations (RTI)	RTI Monitor		Not Affected		RTI Statement			12/16/2021
Red Hat	Red Hat JBoss Enterprise Application Platform	7	Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	Maven Patch - Affects only the Mavenized distribution. Container, Zip and RPM distro aren't affected.		Dec/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Red Hat	Red Hat Process Automation	7	Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	Maven Patch - Affects only the Mavenized distribution. Container, Zip and RPM distro aren't affected.		Dec/21/2021
Red Hat	Red Hat CodeReady Studio	12.21.0	Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	CRS 12.21.1 Patch		Dec/21/2021
Red Hat	Red Hat Data Grid	8	Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	RHSA-2021:5132		Dec/21/2021
Red Hat	Red Hat Integration Camel K		Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	RHSA-2021:5130		Dec/21/2021
Red Hat	Red Hat Integration Camel Quarkus		Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	RHSA-2021:5126		Dec/21/2021
Red Hat	Red Hat JBoss A-MQ Streaming		Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	RHSA-2021:5138		Dec/21/2021
Red Hat	Red Hat JBoss Fuse	7	Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	RHSA-2021:5134		Dec/21/2021
Red Hat	Red Hat Vert.X	4	Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	RHSA-2021:5093		Dec/21/2021
Red Hat OpenShift Container Platform 3.11	openshift3/ose-logging-elasticsearch5		Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	RHSA-2021:5094		Dec/21/2021
Red Hat OpenShift Container Platform 4	openshift4/ose-logging-elasticsearch6		Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	Please refer to Red Hat Customer Portal to find the right errata for your version.		Dec/21/2021
Red Hat OpenShift Container Platform 4	openshift4/ose-metering-hive		Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	Please refer to Red Hat Customer Portal to find the right errata for your version.		Dec/21/2021
Red Hat OpenShift Container Platform 4	openshift4/ose-metering-presto		Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	Please refer to Red Hat Customer Portal to find the right errata for your version.		Dec/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Red Hat OpenShift Logging	logging-elasticsearch6-container		Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	Please refer to Red Hat Customer Portal to find the right errata for your version.		Dec/21/2021
Red Hat	Red Hat Single Sign-On	7	Not Affected		CVE-2021-44228- Red Hat Customer Portal			Dec/21/2021
Red Hat	Red Hat Enterprise Linux	6	Not Affected		CVE-2021-44228- Red Hat Customer Portal			Dec/20/2021
Red Hat	Red Hat Enterprise Linux	7	Not Affected		CVE-2021-44228- Red Hat Customer Portal			Dec/20/2021
Red Hat	Red Hat Enterprise Linux	8	Not Affected		CVE-2021-44228- Red Hat Customer Portal			Dec/20/2021
Red Hat	Red Hat build of Quarkus		Not Affected		CVE-2021-44228- Red Hat Customer Portal			Dec/20/2021
Red Hat	Red Hat Decision Manager	7	Not Affected		CVE-2021-44228- Red Hat Customer Portal			Dec/20/2021
Red Hat Software Collections	rh-java-common-log4j		Not Affected		CVE-2021-44228- Red Hat Customer Portal			Dec/21/2021
Red Hat Software Collections	rh-maven35-log4j12		Not Affected		CVE-2021-44228- Red Hat Customer Portal			Dec/21/2021
Red Hat Software Collections	rh-maven36-log4j12		Not Affected		CVE-2021-44228- Red Hat Customer Portal			Dec/21/2021
Red Hat	log4j-core		Not Affected		CVE-2021-44228- Red Hat Customer Portal			Dec/21/2021
Red Hat	Satellite 5		Not Affected		CVE-2021-44228- Red Hat Customer Portal			Dec/21/2021
Red Hat	Spacewalk		Not Affected		CVE-2021-44228- Red Hat Customer Portal			Dec/21/2021
Red Hat	Red Hat JBoss Enterprise Application Platform Expansion Pack	7	Not Affected		CVE-2021-44228- Red Hat Customer Portal			Dec/20/2021
Red Hat OpenStack Platform 13 (Queens)	opendaylight		Affected	No	CVE-2021-44228- Red Hat Customer Portal	End of Life		Dec/21/2021
Red5Pro					Red5Pro Link			
RedGate					RedGate Link			
ResMed	myAir		Not Affected		ResMed Advisory Link			12/21/2021
ResMed	AirView		Not Affected		ResMed Advisory Link			12/21/2021
Redis					Redis Link			
Reiner SCT					Reiner SCT Forum			
ReportURI					ReportURI Link			
Respondus					Respondus Support Link	This advisory is available to customers only and has not been reviewed by CISA		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Revenera / Flexera					Revenera / Flexera Community Link			
Ricoh					Ricoh Link			
RingCentral					RingCentral Security Bulletin			
Riverbed					Riverbed Support Link			
Rockwell Automation	FactoryTalk Analytics DataFlowML	4.00.00	Affected	Under development	PN1579 - Log4Shell Vulnerability Notice			12/15/2021
Rockwell Automation	FactoryTalk Analytics DataView	3.03.00	Affected	Under development	PN1579 - Log4Shell Vulnerability Notice			12/15/2021
Rockwell Automation	Industrial Data Center	Gen 1, Gen 2, Gen 3, Gen 3.5	Fixed	Follow the mitigation instructions outlined by VMware in VMSA-2021-0028	PN1579 - Log4Shell Vulnerability Notice			12/15/2021
Rockwell Automation	MES EIG	3.03.00	Affected	No, product discontinued	PN1579 - Log4Shell Vulnerability Notice	Customers should upgrade to EIG Hub if possible or work with their local representatives about alternative solutions.		12/15/2021
Rockwell Automation	VersaVirtual	Series A	Fixed	Follow the mitigation instructions outlined by VMware in VMSA-2021-0028	PN1579 - Log4Shell Vulnerability Notice			12/15/2021
Rockwell Automation	Warehouse Management	4.01.00, 4.02.00, 4.02.01, 4.02.02	Affected	Under development	PN1579 - Log4Shell Vulnerability Notice			12/15/2021
Rollbar					Rollbar Blog Post			
Rosette.com					Rosette.com Support Link			
RSA	SecurID Authentication Manager		Not Affected					
RSA	SecurID Authentication Manager Prime		Not Affected					
RSA	SecurID Authentication Manager WebTier		Not Affected					
RSA	SecurID Governance and Lifecycle		Not Affected					
RSA	SecurID Governance and Lifecycle Cloud		Not Affected					
RSA	SecurID Identity Router		Not Affected					
RSA Netwitness					RSA Netwitness Community Link			
Rstudioapi	Rstudioapi	0.13	Not Affected		https://github.com/rstudio/rstudioapi			12/21/2021
Rubrik					Rubrik Support Link	This advisory is available to customers only and has not been reviewed by CISA		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Ruckus	Virtual SmartZone (vSZ)	5.1 to 6.0	Affected		Ruckus Wireless (support.ruckuswireless.com)			12/13/2021
RunDeck by PagerDuty					RunDeck Docs Link			
PagerDuty	PagerDuty SaaS		Fixed		PagerDuty Log4j Zero-Day Vulnerability Updates	We currently see no evidence of compromises on our platform. Our teams continue to monitor for new developments and for impacts on sub-processors and dependent systems. PagerDuty SaaS customers do not need to take any additional action for their PagerDuty SaaS environment		12/21/2021
Runecast	Runecast Analyzer	6.0.3	Fixed	Yes	Runecast Release notes			
SAE-IT					SAE-IT News Link			
SAFE FME Server					SAFE FME Server Community Link			
SAGE					SAGE Announcement Link			
SailPoint					SailPoint Community Link	This advisory is available to customers only and has not been reviewed by CISA		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Salesforce	Analytics Cloud		Affected		Salesforce Statement	“Analytics Cloud is reported to be affected by CVE-2021-44228. Services have been updated to mitigate the issues identified in CVE-2021-44228 and we are executing our final validation steps.”		12/15/2021
Salesforce	B2C Commerce Cloud		Affected		Salesforce Statement	“B2C Commerce Cloud is reported to be affected by CVE-2021-44228. The service is being updated to remediate the vulnerability identified in CVE-2021-44228.”		12/15/2021
Salesforce	ClickSoftware (As-a-Service)		Affected		Salesforce Statement	“ClickSoftware (As-a-Service) is reported to be affected by CVE-2021-44228. The service is being updated to remediate the vulnerability identified in CVE-2021-44228.”		12/15/2021
Salesforce	ClickSoftware (On-Premise)		Unknown		Salesforce Statement	“Please contact Customer Support.”		12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Salesforce	Community Cloud		Affected		Salesforce Statement	"Community Cloud is reported to be affected by CVE-2021-44228. The service is being updated to remediate the vulnerability identified in CVE-2021-44228."		12/15/2021
Salesforce	Data.com		Affected		Salesforce Statement	"Data.com is reported to be affected by CVE-2021-44228. The service has a mitigation in place and is being updated to remediate the vulnerability identified in CVE-2021-44228."		12/15/2021
Salesforce	DataLoader	<=53.0.0	Fixed		Vendor Link			12/22/2021
Salesforce	Datorama		Affected		Salesforce Statement	"Datorama is reported to be affected by CVE-2021-44228. The service has a mitigation in place and is being updated to remediate the vulnerability identified in CVE-2021-44228."		12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Salesforce	Evergage (Interaction Studio)		Affected		Salesforce Statement	"Evergage (Interaction Studio) is reported to be affected by CVE-2021-44228. Services have been updated to mitigate the issues identified in CVE-2021-44228 and we are executing our final validation steps."		12/15/2021
Salesforce	Force.com		Affected		Salesforce Statement	"Force.com is reported to be affected by CVE-2021-44228. The service is being updated to remediate the vulnerability identified in CVE-2021-44228."		12/15/2021
Salesforce	Heroku		Not Affected		Salesforce Statement	"Heroku is reported to not be affected by CVE-2021-44228; no further action is necessary at this time."		12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Salesforce	Marketing Cloud		Affected		Salesforce Statement	“Marketing Cloud is reported to be affected by CVE-2021-44228. The service is being updated to remediate the vulnerability identified in CVE-2021-44228.”		12/15/2021
Salesforce	MuleSoft (Cloud)		Affected		Salesforce Statement	“MuleSoft (Cloud) is reported to be affected by CVE-2021-44228. The service is being updated to remediate the vulnerability identified in CVE-2021-44228.”		12/15/2021
Salesforce	MuleSoft (On-Premise)		Unknown		Salesforce Statement	“Please contact Customer Support.”		12/15/2021
Salesforce	Pardot		Affected		Salesforce Statement	“Pardot is reported to be affected by CVE-2021-44228. The service is being updated to remediate the vulnerability identified in CVE-2021-44228.”		12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Salesforce	Sales Cloud		Affected		Salesforce Statement	“Sales Cloud is reported to be affected by CVE-2021-44228. The service is being updated to remediate the vulnerability identified in CVE-2021-44228.”		12/15/2021
Salesforce	Service Cloud		Affected		Salesforce Statement	“Service Cloud is reported to be affected by CVE-2021-44228. The service is being updated to remediate the vulnerability identified in CVE-2021-44228.”		12/15/2021
Salesforce	Slack		Affected		Salesforce Statement	“Slack is reported to be affected by CVE-2021-44228. The service has a mitigation in place and is being updated to remediate the vulnerability identified in CVE-2021-44228.”		12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Salesforce	Social Studio		Affected		Salesforce Statement	"Social Studio is reported to be affected by CVE-2021-44228. The service has a mitigation in place and is being updated to remediate the vulnerability identified in CVE-2021-44228."		12/15/2021
Salesforce	Tableau (On-Premise)	< 2021.4.1	Fixed		Salesforce Statement	Fixed in 2021.4.1		12/16/2021
Salesforce	Tableau (Online)		Affected		Salesforce Statement	"Tableau (Online) is reported to be affected by CVE-2021-44228. The service is being updated to remediate the vulnerability identified in CVE-2021-44228."		12/15/2021
Sangoma					Sangoma Community Link			
SAP					https://support.sap.com/content/dam/support/en_us/library/ssp/my-support/trust-center/sap-tc-01-5025.pdf	This advisory is available to customers only and has not been reviewed by CISA		12/17/2021
SAP Advanced Platform					SAP Advanced Platform Support Link	This advisory is available to customers only and has not been reviewed by CISA		12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
SAP BusinessObjects					CVE-2021-44228 - Impact of Log4j vulnerability on SAP BusinessObjects SAP BusinessObjects Support Link	The support document is available to customers only and has not been reviewed by CISA		12/17/2021
SAS					SAS Support Link			
SASSAFRAS					SASSAFRAS Link			
Savignano software solutions					Savignano Link			
SBT	SBT	<1.5.6	Affected	Yes	Release 1.5.7 · sbt/sbt(github.com)			12/15/2021
ScaleComputing					ScaleComputing Community Link	This advisory is available to customers only and has not been reviewed by CISA		
ScaleFusion MobileLock Pro					ScaleFusion MobileLock Pro Help			
Schneider Electric	EcoStruxure IT Gateway	V1.5.0 to V1.13.0	Fixed	Yes	EcoStruxure Link			12/20/2021
Schneider Electric	EcoStruxure IT Expert	Cloud	Fixed	Yes				12/20/2021
Schneider Electric	Facility Expert Small Business	Cloud	Fixed	Yes	SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	Wiser by SE platform	Cloud	Fixed	Yes				12/20/2021
Schneider Electric	EASYFIT	Current software and earlier	Affected		SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	Ecoreal XL	Current software and earlier	Affected		SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	Eurotherm Data Reviewer	V3.0.2 and prior	Affected		SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	MSE	Current software and earlier	Affected		SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	NetBotz750/755	Software versions 5.0 through 5.3.0	Affected		SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	NEW630	Current software and earlier	Affected		SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	SDK BOM	Current software and earlier	Affected		SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	SDK-Docgen	Current software and earlier	Affected		SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	SDK-TNC	Current software and earlier	Affected		SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	SDK-UMS	Current software and earlier	Affected		SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	SDK3D2DRenderer	Current software and earlier	Affected		SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	SDK3D360Widget	Current software and earlier	Affected		SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	Select and Config DATA	Current software and earlier	Affected		SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	SNC-API	Current software and earlier	Affected		SE Cybersecurity Best Practices			12/20/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Schneider Electric	SNC-CMM	Current software and earlier	Affected		SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	SNCSEMTECH	Current software and earlier	Affected		SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	SPIMV3	Current software and earlier	Affected		SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	SWBEditor	Current software and earlier	Affected		SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	SWBEngine	Current software and earlier	Affected		SE Cybersecurity Best Practices			12/20/2021
Schweitzer Engineering Laboratories			Not Affected		SEL Advisory Link			12/21/2021
SCM Manager					SCM Manager Link			
ScreenBeam					ScreenBeam Article			
SDL worldServer					SDL worldServer Link			
Seagull Scientific					Seagull Scientific Support Link			
SecurePoint					SecurePoint News Link			
Security Onion					Security Onion Blog Post			
Seeburger					Seeburger Service Desk Link	This advisory is avaiable to customers only and has not been reviewed by CISA		
SentinelOne					SentinelOne Blog Post			
Sentry					Sentry Blog Post			
SEP					SEP Support Link			
Server Eye					Server Eye Blog Post			
ServiceNow					ServiceNow Support Link			
Shibboleth					Shibboleth Announcement			
Shibboleth	All Products	Identity Provider>=3.0, All other software versions	Not Affected		Log4j CVE (non)-impact			12/10/2021
Shopify					Shopify Community Link			
Siebel					Siebel Link			
Siemens	Affected Products				pdf, CSAF	Siemens requests: See pdf for the complete list of affected products, CSAF for automated parsing of data		12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens	Affected Products				pdf, CSAF	Siemens requests: See pdf for the complete list of affected products, CSAF for automated parsing of data		12/19/2021
Siemens Energy	Affected Products				pdf, CSAF	Siemens requests: See pdf for the complete list of affected products, CSAF for automated parsing of data		12/21/2021
Siemens Energy	Affected Products				pdf, CSAF	Siemens requests: See pdf for the complete list of affected products, CSAF for automated parsing of data		12/20/2021
Siemens Energy	Affected Products				pdf, CSAF	Siemens requests: See pdf for the complete list of affected products, CSAF for automated parsing of data		12/16/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens Healthineers	ATELLICA DATA MANAGER v1.1.1 / v1.2.1 / v1.3.1		Affected	See Notes	Siemens Healthineers	If you have determined that your Atellica Data Manager has a "Java communication engine" service, and you require an immediate mitigation, then please contact your Siemens Customer Care Center or your local Siemens technical support representative.		12/22/2021
Siemens Healthineers	CENTRALINK v16.0.2 / v16.0.3		Affected	See Notes	Siemens Healthineers	If you have determined that your CentraLink has a "Java communication engine" service, and you require a mitigation, then please contact your Siemens Customer Care Center or your local Siemens technical support representative.		12/22/2021
Siemens Healthineers	DICOM Proxy VB10A		Affected	See Notes	Siemens Healthineers	Workaround: remove the vulnerable class from the .jar file		12/22/2021
Siemens Healthineers	Somatom Scope Som5 VC50		Affected	See Notes	Siemens Healthineers	evaluation ongoing		12/22/2021
Siemens Healthineers	Somatom Emotion Som5 VC50		Affected	See Notes	Siemens Healthineers	evaluation ongoing		12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens Healthineers	go.All, Som10 VA20 / VA30 / VA40		Affected	See Notes	Siemens Healthineers	Workaround: In the meantime, we recommend preventing access to port 8090 from other devices by configuration of the hospital network.		12/22/2021
Siemens Healthineers	go.Fit, Som10 VA30		Affected	See Notes	Siemens Healthineers	Workaround: In the meantime, we recommend preventing access to port 8090 from other devices by configuration of the hospital network.		12/22/2021
Siemens Healthineers	go.Now, Som10 VA10 / VA20 / VA30 / VA40		Affected	See Notes	Siemens Healthineers	Workaround: In the meantime, we recommend preventing access to port 8090 from other devices by configuration of the hospital network.		12/22/2021
Siemens Healthineers	go.Open Pro, Som10 VA30 / VA40		Affected	See Notes	Siemens Healthineers	Workaround: In the meantime, we recommend preventing access to port 8090 from other devices by configuration of the hospital network.		12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens Healthineers	go.Sim, Som10 VA30 / VA40		Affected	See Notes	Siemens Healthineers	Workaround: In the meantime, we recommend preventing access to port 8090 from other devices by configuration of the hospital network.		12/22/2021
Siemens Healthineers	go.Top, Som10 VA20 / VA20A_SP5 / VA30 / VA40		Affected	See Notes	Siemens Healthineers	Workaround: In the meantime, we recommend preventing access to port 8090 from other devices by configuration of the hospital network.		12/22/2021
Siemens Healthineers	go.Up, Som10 VA10 / VA20 / VA30 / VA40		Affected	See Notes	Siemens Healthineers	Workaround: In the meantime, we recommend preventing access to port 8090 from other devices by configuration of the hospital network.		12/22/2021
Siemens Healthineers	MAGNETOM AERA 1,5T, MAGNETOM PRISMA, MAGNETOM PRISMA FIT, MAGNETOM SKYRA 3T NUMARIS/X VA30A		Affected	See Notes	Siemens Healthineers	LOG4J is used in the context of the help system. Workaround: close port 8090 for standalone systems. Setup IP whitelisting for "need to access" systems to network port 8090 in case a second console is connected.		12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens Healthineers	MAGNETOM Altea NUMARIS/X VA20A		Affected	See Notes	Siemens Healthineers	LOG4J is used in the context of the help system. Workaround: close port 8090 for standalone systems. Setup IP whitelisting for “need to access” systems to network port 8090 in case a second console is connected.		12/22/2021
Siemens Healthineers	MAGNETOM ALTEA, MAGNETOM LUMINA, MAGNETOM SOLA, MAGNETOM VIDA NUMARIS/X VA31A		Affected	See Notes	Siemens Healthineers	LOG4J is used in the context of the help system. Workaround: close port 8090 for standalone systems. Setup IP whitelisting for “need to access” systems to network port 8090 in case a second console is connected.		12/22/2021
Siemens Healthineers	MAGNETOM Amira NUMARIS/X VA12M		Affected	See Notes	Siemens Healthineers	LOG4J is used in the context of the help system. Workaround: close port 8090 for standalone systems. Setup IP whitelisting for “need to access” systems to network port 8090 in case a second console is connected.		12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens Healthineers	MAGNETOM Free.Max NUMARIS/X VA40		Affected	See Notes	Siemens Healthineers	LOG4J is used in the context of the help system. Workaround: close port 8090 for standalone systems. Setup IP whitelisting for "need to access" systems to network port 8090 in case a second console is connected.		12/22/2021
Siemens Healthineers	MAGNETOM Lumina NUMARIS/X VA20A		Affected	See Notes	Siemens Healthineers	LOG4J is used in the context of the help system. Workaround: close port 8090 for standalone systems. Setup IP whitelisting for "need to access" systems to network port 8090 in case a second console is connected.		12/22/2021
Siemens Healthineers	MAGNETOM Sempra NUMARIS/X VA12M		Affected	See Notes	Siemens Healthineers	LOG4J is used in the context of the help system. Workaround: close port 8090 for standalone systems. Setup IP whitelisting for "need to access" systems to network port 8090 in case a second console is connected.		12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens Healthineers	MAGNETOM Sola fit NUMARIS/X VA20A		Affected	See Notes	Siemens Healthineers	LOG4J is used in the context of the help system. Workaround: close port 8090 for standalone systems. Setup IP whitelisting for “need to access” systems to network port 8090 in case a second console is connected.		12/22/2021
Siemens Healthineers	MAGNETOM Sola NUMARIS/X VA20A		Affected	See Notes	Siemens Healthineers	LOG4J is used in the context of the help system. Workaround: close port 8090 for standalone systems. Setup IP whitelisting for “need to access” systems to network port 8090 in case a second console is connected.		12/22/2021
Siemens Healthineers	MAGNETOM Vida fit NUMARIS/X VA20A		Affected	See Notes	Siemens Healthineers	LOG4J is used in the context of the help system. Workaround: close port 8090 for standalone systems. Setup IP whitelisting for “need to access” systems to network port 8090 in case a second console is connected.		12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens Healthineers	MAGNETOM Vida NUMARIS/X VA10A* / VA20A		Affected	See Notes	Siemens Healthineers	LOG4J is used in the context of the help system. Workaround: close port 8090 for standalone systems. Setup IP whitelisting for “need to access” systems to network port 8090 in case a second console is connected.		12/22/2021
Siemens Healthineers	Syngo Carbon Space VA10A / VA10A-CUT2 / VA20A		Affected	See Notes	Siemens Healthineers	Workaround: remove the vulnerable class from the .jar file		12/22/2021
Siemens Healthineers	Syngo MobileViewer VA10A		Affected	See Notes	Siemens Healthineers	The vulnerability will be patch/mitigated in upcoming releases/patches.		12/22/2021
Siemens Healthineers	syngo Plaza VB20A / VB20A_HF01 - HF07 / VB30A / VB30A_HF01 / VB30A_HF02 / VB30B / VB30C / VB30C_HF01 - HF06 / VB30C_HF91		Affected	See Notes	Siemens Healthineers	Workaround: remove the vulnerable class from the .jar file		12/22/2021
Siemens Healthineers	syngo Workflow MLR VB37A / VB37A_HF01 / VB37A_HF02 / VB37B / VB37B_HF01 - HF07 / VB37B_HF93 / VB37B_HF94 / VB37B_HF96		Affected	See Notes	Siemens Healthineers	Please contact your Customer Service to get support on mitigating the vulnerability.		12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens Healthineers	syngo.via VB20A / VB20A_HF01 - HF08 / VB20A_HF91 / VB20B / VB30A / VB30A_HF01 - VB30A_HF08 / VB30A_HF91VB30B / VB30B_HF01 / VB40A / VB40A_HF01 - HF02 /VB40B / VB40B_HF01 - HF05 / VB50A / VB50A_CUT / VB50A_D4VB50B / VB50B_HF01 - HF03 / VB60A / VB60A_CUT / VB60A_D4 / VB60A_HF01		Affected	See Notes	Siemens Healthineers	Workaround: remove the vulnerable class from the .jar file		12/22/2021
Siemens Healthineers	SENSIS DMCC / DMCM / TS / VM / PPWS / DS VD12A		Affected	See Notes	Siemens Healthineers	evaluation ongoing		12/22/2021
Siemens Healthineers	Cios Select FD/I.I. VA21 / VA21-S3P		Affected	See Notes	Siemens Healthineers	evaluation ongoing		12/22/2021
Siemens Healthineers	Cios Flow S1 / Alpha / Spin VA30		Affected	See Notes	Siemens Healthineers	evaluation ongoing		12/22/2021
Siemens Healthineers	syngo.via WebViewer VA13B / VA20A / VA20B		Affected	See Notes	Siemens Healthineers	Workaround: remove the vulnerable class from the .jar file		12/22/2021
Siemens Healthineers	X.Ceed Somaris 10 VA40*		Affected	See Notes	Siemens Healthineers	Workaround: In the meantime, we recommend preventing access to port 8090 from other devices by configuration of the hospital network.		12/22/2021
Siemens Healthineers	X.Cite Somaris 10 VA30/*VA40*		Affected	See Notes	Siemens Healthineers	Workaround: In the meantime, we recommend preventing access to port 8090 from other devices by configuration of the hospital network.		12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Sierra Wireless					Sierra Wireless Security Bulletin			
Signald					Signald Gitlab			
Silver Peak	Orchestrator, Silver Peak GMS		Affected	No	Security Advisory Notice Apache	Customer managed Orchestrator and legacy GMS products are affected by this vulnerability. This includes on-premise and customer managed instances running in public cloud services such as AWS, Azure, Google, or Oracle Cloud. See Corrective Action Required for details about how to mitigate this exploit.		12/14/2021
SingleWire					SingleWire Support Link	This advisory is available to customers only and has not been reviewed by CISA		
Sitecore					Sitecore Support Link			
Skillable					Skillable Link			
SLF4J					SLF4J Link			
Slurm	Slurm	20.11.8	Not Affected		https://slurm.schedmd.com/documentation.html			12/21/2021
SmartBear					SmartBear Link			
SmileCDR					SmileCDR Blog Post			
Snakemake	Snakemake	6.12.1	Not Affected		https://snakemake.readthedocs.io/en/stable/			12/21/2021
Sn0m					Sn0m Link			
Snowflake			Not Affected		Snowflake Community Link			
Snyk	Cloud Platform		Not Affected		Snyk Updates			
Software AG					Software AG			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
SolarWinds	Database Performance Analyzer (DPA)	2021.1.x, 2021.3.x, 2022.1.x	Affected	No	Apache Log4j Critical Vulnerability (CVE-2021-44228) Database Performance Analyzer (DPA) and the Apache Log4j Vulnerability (CVE-2021-44228)	Workarounds available, hotfix under development		12/14/2021
SolarWinds	Server & Application Monitor (SAM)	SAM 2020.2.6 and later	Affected	No	Apache Log4j Critical Vulnerability (CVE-2021-44228) Server & Application Monitor (SAM) and the Apache Log4j Vulnerability (CVE-2021-44228)	Workarounds available, hotfix under development		12/14/2021
SonarSource					SonarSource			
Sonatype					Sonatype Vulnerability Statement			
SonicWall	Capture Client & Capture Client Portal		Not Affected		Sonic Wall Security Advisory	Log4j2 not used in the Capture Client.		12/12/2021
SonicWall	Access Points		Not Affected		Security Advisory (sonicwall.com)	Log4j2 not used in the SonicWall Access Points		12/12/2021
SonicWall	Analytics		Under Investigation		Security Advisory (sonicwall.com)	Under Review		12/12/2021
SonicWall	Analyzer		Under Investigation		Security Advisory (sonicwall.com)	Under Review		12/12/2021
SonicWall	Capture Security Appliance		Not Affected		Security Advisory (sonicwall.com)	Log4j2 not used in the Capture Security appliance.		12/12/2021
SonicWall	CAS		Under Investigation		Security Advisory (sonicwall.com)	Under Review		12/12/2021
SonicWall	Email Security		Affected	Yes	Security Advisory (sonicwall.com)	ES 10.0.11 and earlier versions are impacted		12/17/2021
SonicWall	Gen5 Firewalls (EOS)		Not Affected		Security Advisory (sonicwall.com)	Log4j2 not used in the appliance.		12/12/2021
SonicWall	Gen6 Firewalls		Not Affected		Security Advisory (sonicwall.com)	Log4j2 not used in the appliance.		12/12/2021
SonicWall	Gen7 Firewalls		Not Affected		Security Advisory (sonicwall.com)	Log4j2 not used in the appliance.		12/12/2021
SonicWall	GMS		Under Investigation		Security Advisory (sonicwall.com)	Under Review		12/12/2021
SonicWall	MSW		Not Affected		Security Advisory (sonicwall.com)	Mysonicwall service doesn't use Log4j		12/12/2021
SonicWall	NSM		Not Affected		Security Advisory (sonicwall.com)	NSM On-Prem and SaaS doesn't use a vulnerable version		12/12/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
SonicWall	SMA 100		Not Affected		Security Advisory (sonicwall.com)	Log4j2 not used in the SMA100 appliance.		12/12/2021
SonicWall	SMA 1000		Not Affected		Security Advisory (sonicwall.com)	Version 12.1.0 and 12.4.1 doesn't use a vulnerable version		12/12/2021
SonicWall	SonicCore		Not Affected		Security Advisory (sonicwall.com)	SonicCore doesn't use a Log4j2		12/12/2021
SonicWall	SonicWall Switch		Not Affected		Security Advisory (sonicwall.com)	Log4j2 not used in the SonicWall Switch.		12/12/2021
SonicWall	WAF		Under Investigation		Security Advisory (sonicwall.com)	Under Review		12/12/2021
SonicWall	WNM		Not Affected		Security Advisory (sonicwall.com)	Log4j2 not used in the WNM.		12/12/2021
SonicWall	WXA		Not Affected		Security Advisory (sonicwall.com)	WXA doesn't use a vulnerable version		12/12/2021
Sophos	Cloud Optix		Fixed		Advisory: Log4J zero-day vulnerability AKA Log4Shell (CVE-2021-44228) Sophos	Users may have noticed a brief outage around 12:30 GMT as updates were deployed. There was no evidence that the vulnerability was exploited and to our knowledge no customers are impacted.		12/12/2021
Sophos	Reflexion		Not Affected		Advisory: Log4J zero-day vulnerability AKA Log4Shell (CVE-2021-44228) Sophos	Reflexion does not run an exploitable configuration.		12/12/2021
Sophos	SG UTM (all versions)		Not Affected		Advisory: Log4J zero-day vulnerability AKA Log4Shell (CVE-2021-44228) Sophos	Sophos SG UTM does not use Log4j.		12/12/2021
Sophos	SG UTM Manager (SUM) (all versions)	All versions	Not Affected		Advisory: Log4J zero-day vulnerability AKA Log4Shell (CVE-2021-44228) Sophos	SUM does not use Log4j.		12/12/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Sophos	Sophos Central		Not Affected		Advisory: Log4J zero-day vulnerability AKA Log4Shell (CVE-2021-44228) Sophos	Sophos Central does not run an exploitable configuration.		12/12/2021
Sophos	Sophos Firewall (all versions)		Not Affected		Advisory: Log4J zero-day vulnerability AKA Log4Shell (CVE-2021-44228) Sophos	Sophos Firewall does not use Log4j.		12/12/2021
Sophos	Sophos Home		Not Affected		Advisory: Log4J zero-day vulnerability AKA Log4Shell (CVE-2021-44228) Sophos	Sophos Home does not use Log4j.		12/12/2021
Sophos	Sophos Mobile		Not Affected		Advisory: Log4J zero-day vulnerability AKA Log4Shell (CVE-2021-44228) Sophos	Sophos Mobile (in Central, SaaS, and on-premises) does not run an exploitable configuration.		12/12/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Sophos	Sophos Mobile EAS Proxy	< 9.7.2	Affected	No	Advisory: Log4J zero-day vulnerability AKA Log4Shell (CVE-2021-44228) Sophos	The Sophos Mobile EAS Proxy, running in Traffic Mode, is affected. Customers will need to download and install version 9.7.2, available from Monday December 13, 2021, on the same machine where it is currently running. PowerShell mode is not affected. Customers can download the Standalone EAS Proxy Installer version 9.7.2 from the Sophos website.		12/12/2021
Sophos	Sophos ZTNA		Not Affected		Advisory: Log4J zero-day vulnerability AKA Log4Shell (CVE-2021-44228) Sophos	Sophos ZTNA does not use Log4j.		12/12/2021
SOS Berlin					SOS Berlin Link			
Spambrella					Spambrella FAQ Link			
Spigot					Spigot Security Release			
Splunk	Splunk Add-On for Java Management Extensions App ID 2647	5.2.0 and older	Affected	CVE-2021-44228: 5.2.1 CVE-2021-45046: 5.2.2 CVE-2021-45105: not applicable due to configuration parameters	Splunk Security Advisory for Apache Log4j (CVE-2021-44228 and CVE-2021-45046)			9:25 am PT, 12/21/21
Splunk	Splunk Splunk Add-On for JBoss App ID 2954	3.0.0 and older	Affected	CVE-2021-44228: 3.0.1 CVE-2021-45046: 3.0.2 CVE-2021-45105: not applicable due to configuration parameters	Splunk Security Advisory for Apache Log4j (CVE-2021-44228 and CVE-2021-45046)			9:25 am PT, 12/21/21
Splunk	Splunk Add-On for Tomcat App ID 2911	3.0.0 and older	Affected	CVE-2021-44228: 3.0.1 CVE-2021-45046: 3.0.2 CVE-2021-45105: not applicable due to configuration parameters	Splunk Security Advisory for Apache Log4j (CVE-2021-44228 and CVE-2021-45046)			9:25 am PT, 12/21/21

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Splunk	Data Stream Processor	DSP 1.0.x, DSP 1.1.x, DSP 1.2.x	Affected	Version 1.0.0 and 1.0.1 are out of support and will not receive a patch. Customers on supported versions (> 1.1.0) should patch to the following versions: CVE-2021-44228: 1.2.1-patch02, 1.2.2-patch02 CVE-2021-45046: 1.2.1-patch02, 1.2.2-patch02 CVE-2021-45105: not applicable due to configuration parameters	Splunk Security Advisory for Apache Log4j (CVE-2021-44228 and CVE-2021-45046)			9:25 am PT, 12/21/21
Splunk	IT Essentials Work App ID 5403	4.11, 4.10.x (Cloud only), 4.9.x	Affected	CVE-2021-44228: 4.11.1, 4.10.3, 4.9.5 CVE-2021-45046: 4.11.2, 4.10.4, 4.9.6, 4.7.4 CVE-2021-45105: not applicable due to configuration parameters	Splunk Security Advisory for Apache Log4j (CVE-2021-44228 and CVE-2021-45046)			9:25 am PT, 12/21/21
Splunk	IT Service Intelligence (ITSI) App ID 1841	4.11.0, 4.10.x (Cloud only), 4.9.x, 4.8.x (Cloud only), 4.7.x, 4.6.x, 4.5.x	Affected	CVE-2021-44228: 4.11.1, 4.10.3, 4.9.5, 4.7.3 CVE-2021-45046: 4.11.2, 4.10.4, 4.9.6, 4.7.4 CVE-2021-45105: not applicable due to configuration parameters	Splunk Security Advisory for Apache Log4j (CVE-2021-44228 and CVE-2021-45046)			9:25 am PT, 12/21/21
Splunk	Splunk Connect for Kafka	All versions prior to 2.0.4	Affected	CVE-2021-44228: 2.0.4 CVE-2021-45046: 2.0.5 CVE-2021-45105: 2.0.6	Splunk Security Advisory for Apache Log4j (CVE-2021-44228 and CVE-2021-45046)			9:25 am PT, 12/21/21
Splunk	Splunk Enterprise (including instance types like Heavy Forwarders)	All supported non-Windows versions of 8.1.x and 8.2.x only if DFS is used. See Removing Log4j from Splunk Enterprise below for guidance on unsupported versions.	Affected	CVE-2021-44228: 8.1.7.1, 8.2.3.2 CVE-2021-45046: 8.1.7.2, 8.2.3.3 CVE-2021-45105: not applicable due to configuration parameters	Splunk Security Advisory for Apache Log4j (CVE-2021-44228 and CVE-2021-45046)			9:25 am PT, 12/21/21
Splunk	Splunk Enterprise Amazon Machine Image (AMI)	See Splunk Enterprise	Affected	CVE-2021-44228: 8.2.3.2, 8.1.7.1 published to AWS Marketplace CVE-2021-45046: 8.2.3.3, 8.1.7.2	Splunk Security Advisory for Apache Log4j (CVE-2021-44228 and CVE-2021-45046)			9:25 am PT, 12/21/21
Splunk	Splunk Enterprise Docker Container	See Splunk Enterprise	Affected	CVE-2021-44228: latest, edge, 8.1, 8.1.7.1, 8.2, 8.2.3.2 CVE-2021-45046: latest, edge, 8.1, 8.1.7.2, 8.2, 8.2.3.3 CVE-2021-45105: not applicable due to configuration parameters	Splunk Security Advisory for Apache Log4j (CVE-2021-44228 and CVE-2021-45046)			9:25 am PT, 12/21/21
Splunk	Splunk Logging Library for Java	1.11.0 and older	Affected	CVE-2021-44228: 1.11.1 CVE-2021-45046: 1.11.2	Splunk Security Advisory for Apache Log4j (CVE-2021-44228 and CVE-2021-45046)			9:25 am PT, 12/21/21
Splunk	Splunk OVA for VMWare App ID 3216	4.0.3 and older	Affected	Pending	Splunk Security Advisory for Apache Log4j (CVE-2021-44228 and CVE-2021-45046)			9:25 am PT, 12/21/21
Splunk	Splunk OVA for VMWare Metrics App ID 5096	4.2.1 and older	Affected	Pending	Splunk Security Advisory for Apache Log4j (CVE-2021-44228 and CVE-2021-45046)			9:25 am PT, 12/21/21
Splunk	Splunk VMWare OVA for ITSI App ID 4760	1.1.1 and older	Affected	CVE-2021-44228: TBD CVE-2021-45046: TBD	Splunk Security Advisory for Apache Log4j (CVE-2021-44228 and CVE-2021-45046)			9:25 am PT, 12/21/21
Splunk	Splunk On-call / VictorOps	Current	Affected	CVE-2021-44228: Fixed 12/15 CVE-2021-45046: Fixed 12/20	Splunk Security Advisory for Apache Log4j (CVE-2021-44228 and CVE-2021-45046)			9:25 am PT, 12/21/21
Splunk	Splunk Real User Monitoring	Current	Affected	CVE-2021-44228: Fixed 12/13 CVE-2021-45046: Fixed 12/20	Splunk Security Advisory for Apache Log4j (CVE-2021-44228 and CVE-2021-45046)			9:25 am PT, 12/21/21

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Splunk	Splunk Application Performance Monitoring	Current	Affected	CVE-2021-44228: Fixed 12/13 CVE-2021-45046: Fixed 12/20	Splunk Security Advisory for Apache Log4j (CVE-2021-44228 and CVE-2021-45046)			9:25 am PT, 12/21/21
Splunk	Splunk Infrastructure Monitoring	Current	Affected	CVE-2021-44228: Fixed 12/13 CVE-2021-45046: Fixed 12/20	Splunk Security Advisory for Apache Log4j (CVE-2021-44228 and CVE-2021-45046)			9:25 am PT, 12/21/21
Splunk	Splunk Log Observer	Current	Affected	CVE-2021-44228: Fixed 12/16 CVE-2021-45046: Fixed 12/20	Splunk Security Advisory for Apache Log4j (CVE-2021-44228 and CVE-2021-45046)			9:25 am PT, 12/21/21
Splunk	Splunk Synthetics	Current	Affected	CVE-2021-44228: Fixed 12/10 CVE-2021-45046: Fixed 12/20	Splunk Security Advisory for Apache Log4j (CVE-2021-44228 and CVE-2021-45046)			9:25 am PT, 12/21/21
Splunk	Splunk UBA OVA Software	5.0.3a, 5.0.0	Affected	Pending	Splunk Security Advisory for Apache Log4j (CVE-2021-44228 and CVE-2021-45046)			9:25 am PT, 12/21/21
Sprecher Automation					Sprecher Automation Security Alert			
Spring	Spring Boot		Unknown		https://spring.io/blog/2021/12/10/log4j2-vulnerability-and-spring-boot	Spring Boot users are only affected by this vulnerability if they have switched the default logging system to Log4J2		
Spring Boot					Spring Boot Vulnerability Statement			
StarDog					StarDog			
STERIS	Advantage		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	Advantage Plus		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	DSD Edge		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	EndoDry		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	RapidAER		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	Endora		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	Canexis 1.0		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	ConnectoHIS		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	ScopeBuddy+		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	DSD-201,		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	CER Optima		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	Renatron		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	ConnectAssure Technology		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	SPM Surgical Asset Tracking Software		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	CS-iQ Sterile Processing Workflow		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	AMSCO 2000 SERIES WASHER DISINFECTORS		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	AMSCO 3000 SERIES WASHER DISINFECTORS		Not Affected		STERIS Advisory Link			12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
STERIS	AMSCO 5000 SERIES WASHER DISINFECTORS		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	AMSCO 7000 SERIES WASHER DISINFECTORS		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	RELIANCE 444 WASHER DISINFECTOR		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	RELIANCE SYNERGY WASHER DISINFECTOR		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	RELIANCE VISION 1300 SERIES CART AND UTENSIL WASHER DISINFECTORS		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	RELIANCE VISION MULTI-CHAMBER WASHER DISINFECTOR		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	RELIANCE VISION SINGLE CHAMBER WASHER DISINFECTOR		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	AMSCO 400 MEDIUM STEAM STERILIZER		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	AMSCO 400 SMALL STEAM STERILIZERS		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	AMSCO 600 MEDIUM STEAM STERILIZER		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	AMSCO CENTURY MEDIUM STEAM STERILIZER		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	AMSCO CENTURY SMALL STEAM STERILIZER		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	AMSCO EAGLE 3000 SERIES STAGE 3 STEAM STERILIZERS		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	AMSCO EVOLUTION FLOOR LOADER STEAM STERILIZER		Not Affected		STERIS Advisory Link			12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
STERIS	AMSCO EVOLUTION MEDIUM STEAM STERILIZER		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	CELERITY HP INCUBATOR		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	CELERITY STEAM INCUBATOR		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	VERIFY INCUBATOR FOR ASSERT SELF-CONTAINED BIOLOGICAL INDICATORS		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	SYSTEM 1 endo LIQUID CHEMICAL STERILANT PROCESSING SYSTEM		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	V-PRO 1 LOW TEMPERATURE STERILIZATION SYSTEM		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	V-PRO 1 PLUS LOW TEMPERATURE STERILIZATION SYSTEM		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	V-PRO MAX 2 LOW TEMPERATURE STERILIZATION SYSTEM		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	V-PRO MAX LOW TEMPERATURE STERILIZATION SYSTEM		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	V-PRO S2 LOW TEMPERATURE STERILIZATION SYSTEM		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	SecureCare ProConnect Technical Support Services		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	HexaVue Integration System		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	IDSS Integration System		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	Harmony iQ Integration Systems		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	HexaVue		Not Affected		STERIS Advisory Link			12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
STERIS	Connect Software		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	Harmony iQ Perspectives Image Management System		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	Clarity Software		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	Situational Awareness for Everyone Display (S.A.F.E.)		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	RealView Visual Workflow Management System		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	ReadyTracker		Not Affected		STERIS Advisory Link			12/22/2021
Sterling Order IBM					IBM Statement			
Storagement					Storagement			
StormShield					StormShield Security Alert			
StrangeBee TheHive & Cortex					StrangeBee Statement			
Stratodesk					STratodesk Statement			
Strimzi					Strimzi Statement			
Stripe					Stripe Support			
Styra					Styra Security Notice			
Sumologic					Sumologic Statement			
SumoLogic					Sumologic Release Notes			
Superna EYEGLASS					Superna EYEGLASS Technical Advisory			
Suprema Inc					Suprema Inc			
SUSE					SUSE Statement			
Sweepwidget					Sweepwidget Statement			
Swyx					Swyx Advisory			
Synchro MSP					Synchro MSP Advisory			
Syncplify					Syncplify Advisory			
Synology					Synology Advisory			
Synopsys					Synopsys Advisory			
Syntevo					Syntevo Statement			
SysAid					https://www.sysaid.com/lp/important-update-regarding-apache-log4j			
Sysdig					https://sysdig.com/blog/cve-critical-vulnerability-log4j/			
Tableau	Tableau Server	The following versions and lower: 2021.4, 2021.3.4, 2021.2.5, 2021.1.8, 2020.4.11, 2020.3.14, 2020.2.19, 2020.1.22, 2019.4.25, 2019.3.26, 2019.2.29, 2019.1.29, 2018.3.29	Affected	Yes	Apache Log4j2 vulnerability (Log4shell)			12/22/2021
Tableau	Tableau Desktop	The following versions and lower: 2021.4, 2021.3.4, 2021.2.5, 2021.1.8, 2020.4.11, 2020.3.14, 2020.2.19, 2020.1.22, 2019.4.25, 2019.3.26, 2019.2.29, 2019.1.29, 2018.3.29	Affected	Yes	Apache Log4j2 vulnerability (Log4shell)			12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Tableau	Tableau Prep Builder	The following versions and lower: 22021.4.1, 2021.3.2, 2021.2.2, 2021.1.4, 2020.4.1, 2020.3.3, 2020.2.3, 2020.1.5, 2019.4.2, 2019.3.2, 2019.2.3, 2019.1.4, 2018.3.3	Affected	Yes	Apache Log4j2 vulnerability (Log4shell)			12/22/2021
Tableau	Tableau Public Desktop Client	The following versions and lower: 2021.4	Affected	Yes	Apache Log4j2 vulnerability (Log4shell)			12/22/2021
Tableau	Tableau Reader	The following versions and lower: 2021.4	Affected	Yes	Apache Log4j2 vulnerability (Log4shell)			12/22/2021
Tableau	Tableau Bridge	The following versions and lower: 20214.21.1109.1748, 20213.21.1112.1434, 20212.21.0818.1843, 20211.21.0617.1133, 20204.21.0217.1203, 20203.20.0913.2112, 20202.20.0721.1350, 20201.20.0614.2321, 20194.20.0614.2307, 20193.20.0614.2306, 20192.19.0917.1648, 20191.19.0402.1911, 20183.19.0115.1143	Affected	Yes	Apache Log4j2 vulnerability (Log4shell)			12/22/2021
Talend					https://jira.talendforge.org/browse/TCOMP-2054			
Tanium	All	All versions	Not Affected		Tanium Statement	Tanium does not use Log4j.		12/21/2021
TealiumIQ					TealiumIQ Security Update			
TeamPasswordManager					TeamPasswordManager Blog			
Teamviewer					TeamViewer Bulletin			
Tech Software	OneAegis (f/k/a IRBManager)	All versions	Not Affected		Log4j CVE-2021-44228 Vulnerability Impact Statement	OneAegis does not use Log4j.		12/15/2021
Tech Software	SMART	All versions	Not Affected		Log4j CVE-2021-44228 Vulnerability Impact Statement	SMART does not use Log4j.		12/15/2021
Tech Software	Study Binders	All versions	Not Affected		Log4j CVE-2021-44228 Vulnerability Impact Statement	Study Binders does not use Log4j.		12/15/2021
TechSmith					TechSmith Article			
Telestream					Telestream Bulletin			
Tenable	Tenable.io / Nessus		Not Affected		Tenable log4j Statement	None of Tenable's products are running the version of Log4j vulnerable to CVE-2021-44228 or CVE-2021-45046 at this time		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Thales	CipherTrust Application Data Protection (CADP) – CAPI.net & Net Core		Not Affected		Thales Support			12/17/2021
Thales	CipherTrust Cloud Key Manager (CCKM) Embedded		Not Affected		Thales Support			12/17/2021
Thales	CipherTrust Database Protection		Not Affected		Thales Support			12/17/2021
Thales	CipherTrust Manager		Not Affected		Thales Support			12/17/2021
Thales	CipherTrust Transparent Encryption (CTE/VTE/CTE-U)		Not Affected		Thales Support			12/17/2021
Thales	CipherTrust Vaultless Tokenization (CTS, CT-VL)		Not Affected		Thales Support			12/17/2021
Thales	Data Protection on Demand		Not Affected		Thales Support			12/17/2021
Thales	Data Security Manager (DSM)		Not Affected		Thales Support			12/17/2021
Thales	KeySecure		Not Affected		Thales Support			12/17/2021
Thales	Luna EFT		Not Affected		Thales Support			12/17/2021
Thales	Luna Network, PCIe, Luna USB HSM and backup devices		Not Affected		Thales Support			12/17/2021
Thales	Luna SP		Not Affected		Thales Support			12/17/2021
Thales	ProtectServer HSMs		Not Affected		Thales Support			12/17/2021
Thales	SafeNet Authentication Client		Not Affected		Thales Support			12/17/2021
Thales	SafeNet IDPrime Virtual		Not Affected		Thales Support			12/17/2021
Thales	SafeNet eToken (all products)		Not Affected		Thales Support			12/17/2021
Thales	SafeNet IDPrime(all products)		Not Affected		Thales Support			12/17/2021
Thales	SafeNet LUKS		Not Affected		Thales Support			12/17/2021
Thales	SafeNet ProtectApp (PA) CAPI, .Net & Net Core		Not Affected		Thales Support			12/17/2021
Thales	SafeNet ProtectDB (PDB)		Not Affected		Thales Support			12/17/2021
Thales	SafeNet ProtectV		Not Affected		Thales Support			12/17/2021
Thales	Safenet ProtectFile and ProtectFile-Fuse		Not Affected		Thales Support			12/17/2021
Thales	SafeNet Transform Utility (TU)		Not Affected		Thales Support			12/17/2021
Thales	SafeNet Trusted Access (STA)		Not Affected		Thales Support			12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Thales	SafeNet PKCS#11 and TDE		Not Affected		Thales Support			12/17/2021
Thales	SafeNet SQL EKM		Not Affected		Thales Support			12/17/2021
Thales	SAS on Prem (SPE/PCE)		Not Affected		Thales Support			12/17/2021
Thales	Sentinel EMS Enterprise OnPremise		Not Affected		Thales Support			12/17/2021
Thales	Sentinel ESDaaS		Not Affected		Thales Support			12/17/2021
Thales	Sentinel Up		Not Affected		Thales Support			12/17/2021
Thales	Sentinel RMS		Not Affected		Thales Support			12/17/2021
Thales	Sentinel Connect		Not Affected		Thales Support			12/17/2021
Thales	Sentinel Superdog, SuperPro, UltraPro, SHK		Not Affected		Thales Support			12/17/2021
Thales	Sentinel HASP, Legacy dog, Maze, Hardlock		Not Affected		Thales Support			12/17/2021
Thales	Sentinel Envelope		Not Affected		Thales Support			12/17/2021
Thales	Thales payShield 9000		Not Affected		Thales Support			12/17/2021
Thales	Thales payShield 10k		Not Affected		Thales Support			12/17/2021
Thales	Thales payShield Manager		Not Affected		Thales Support			12/17/2021
Thales	Vormetirc Key Manager (VKM)		Not Affected		Thales Support			12/17/2021
Thales	Vormetric Application Encryption (VAE)		Not Affected		Thales Support			12/17/2021
Thales	Vormetric Protection for Terradata Database (VPTD)		Not Affected		Thales Support			12/17/2021
Thales	Vormetric Tokenization Server (VTS)		Not Affected		Thales Support			12/17/2021
Thales	payShield Monitor		Under Investigation		Thales Support			12/17/2021
Thales	CADP/SafeNet Protect App (PA) - JCE		Affected		Thales Support			12/17/2021
Thales	CipherTrust Batch Data Transformation (BDT) 2.3		Affected		Thales Support			12/17/2021
Thales	CipherTrust Cloud Key Manager (CCKM) Appliance		Affected		Thales Support			12/17/2021
Thales	CipherTrust Vaulted Tokenization (CT-V) / SafeNet Tokenization Manager		Affected		Thales Support			12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Thales	CipherTrust/SafeNet PDBCTL		Affected		Thales Support			12/17/2021
Thales	Crypto Command Center (CCC)		Affected		Thales Support			12/17/2021
Thales	SafeNet Vaultless Tokenization		Affected		Thales Support			12/17/2021
Thales	Sentinel LDK EMS (LDK-EMS)		Affected		Thales Support			12/17/2021
Thales	Sentinel LDKaas (LDK-EMS)		Affected		Thales Support			12/17/2021
Thales	Sentinel EMS Enterprise aaS		Affected		Thales Support			12/17/2021
Thales	Sentinel Professional Services components (both Thales hosted & hosted on-premises by customers)		Affected		Thales Support			12/17/2021
Thales	Sentinel SCL		Affected		Thales Support			12/17/2021
Thales	Thales Data Platform (TDP)(DDC)		Affected		Thales Support			12/17/2021
Thermo-Calc	Thermo-Calc	2022a	Not Affected		Thermo-Calc Advisory Link	Use the program as normal, Install the 2022a patch when available		12/22/2021
Thermo-Calc	Thermo-Calc	2021b	Not Affected		Thermo-Calc Advisory Link	Use the program as normal		12/22/2021
Thermo-Calc	Thermo-Calc	2018b to 2021a	Not Affected		Thermo-Calc Advisory Link	Use the program as normal, delete the Log4j 2 files in the program installation if required, see advisory for instructions.		12/22/2021
Thermo-Calc	Thermo-Calc	2018a and earlier	Not Affected		Thermo-Calc Advisory Link	Use the program as normal		12/22/2021
Thermo Fisher Scientific			Unknown		Thermo Fisher Scientific Advisory Link			12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Thomson Reuters	HighQ Appliance	<3.5	Affected	Yes	https://highqsolutions.zendesk.com	Reported by vendor - Documentation is in vendor's client portal (login required). This advisory is available to customer only and has not been reviewed by CISA.		12/20/2021
ThreatLocker					ThreatLocker Log4j Statement			
ThycoticCentrify	Secret Server	N/A	Not Affected		ThycoticCentrify Products NOT Affected by CVE-2021-44228 Exploit			12/10/21
ThycoticCentrify	Privilege Manager	N/A	Not Affected		ThycoticCentrify Products NOT Affected by CVE-2021-44228 Exploit			12/10/21
ThycoticCentrify	Account Lifecycle Manager	N/A	Not Affected		ThycoticCentrify Products NOT Affected by CVE-2021-44228 Exploit			12/10/21
ThycoticCentrify	Privileged Behavior Analytics	N/A	Not Affected		ThycoticCentrify Products NOT Affected by CVE-2021-44228 Exploit			12/10/21
ThycoticCentrify	DevOps Secrets Vault	N/A	Not Affected		ThycoticCentrify Products NOT Affected by CVE-2021-44228 Exploit			12/10/21
ThycoticCentrify	Connection Manager	N/A	Not Affected		ThycoticCentrify Products NOT Affected by CVE-2021-44228 Exploit			12/10/21
ThycoticCentrify	Password Reset Server	N/A	Not Affected		ThycoticCentrify Products NOT Affected by CVE-2021-44228 Exploit			12/10/21
ThycoticCentrify	Cloud Suite	N/A	Not Affected		ThycoticCentrify Products NOT Affected by CVE-2021-44228 Exploit			12/10/21
Tibco					Tibco Support Link			
Top Gun Technology (TGT)					TGT Bulletin			
TopDesk					TopDesk Statement			
Topicus Security	Topicus KeyHub	All	Not Affected		Topicus Keyhub Statement			2021-12-20
Topix					Topix Statement			
Tosibox					Tosibox Security Advisory			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
TPLink	Omega Controller	Linux/Windows(all)	Affected	Yes	Statement on Apache Log4j Vulnerability	Update is Beta. Reddit: overwritten vulnerable log4j with 2.15 files as potential workaround. Though that should now be done with 2.16	Tp Community Link,Reddit Link	12/15/2021
TrendMicro	All		Under Investigation		https://success.trendmicro.com/solution/000289940			
Tricentis Tosca					Tricentis Tosca Statement			
Tripwire					Tripwire Log4j Statement			
Trimble	eCognition	10.2.0 Build 4618	Affected	No	Details are shared with active subscribers	Remediation steps provided by Trimble		12/23/2021
TrueNAS					TrueNAS Statement			
Tufin					Tufin Statement			
TYPO3					TYPO3 Statement			
Ubiquiti	UniFi Network Application	6.5.53 & lower versions	Affected	Yes	UniFi Network Application 6.5.54 Ubiquiti Community			
Ubiquiti	UniFi Network Controller	6.5.54 & lower versions	Affected	Yes	UniFi Network Application 6.5.55 Ubiquiti Community		6.5.54 is reported to still be vulnerable. 6.5.55 is the new recommendation for mitigatin log4j vulnerabilities by updating to log4j 2.16.0	12/15/2021
Ubuntu					Ubuntu Security Advisory			
Umbraco					Umbraco Security Advisory			
UniFlow					UniFlow Security Advisory			
Unify ATOS					Unify ATOS Advisory			
Unimus					Unimus Statement			
USSIGNAL MSP					USSIGNAL MSP Statement			
VArmour					VArmour Statement			
Varian	Acuity	All	Under Investigation		Varian Advisory Link			12/22/2021
Varian	DITC	All	Under Investigation		Varian Advisory Link			12/22/2021
Varian	ARIA Connect (Cloverleaf)	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	ARIA oncology information system for Medical Oncology	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	XMediusFax for ARIA oncology information system for Medical Oncology	All	Under Investigation		Varian Advisory Link			12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Varian	ARIA oncology information system for Radiation Oncology	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	ARIA eDOC	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	XMediusFax for ARIA oncology information system for Radiation Oncology	All	Under Investigation		Varian Advisory Link			12/22/2021
Varian	ARIA Radiation Therapy Management System (RTM)	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	Bravos Console	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	Clinac	All	Under Investigation		Varian Advisory Link			12/22/2021
Varian	Cloud Planner	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	DoseLab	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	Eclipse treatment planning software	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	ePeerReview	All	Under Investigation		Varian Advisory Link			12/22/2021
Varian	Ethos	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	FullScale oncology IT solutions	All	Under Investigation		Varian Advisory Link			12/22/2021
Varian	Halcyon system	All	Under Investigation		Varian Advisory Link			12/22/2021
Varian	Identify	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	Information Exchange Manager (IEM)	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	InSightive Analytics	All	Under Investigation		Varian Advisory Link			12/22/2021
Varian	Large Integrated Oncology Network (LION)	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	ICAP	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	Mobius3D platform	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	ProBeam	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	Qumulate	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	Real-time Position Management (RPM)	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	Respiratory Gating for Scanners (RGSC)	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	SmartConnect solution	All	Affected		Varian Advisory Link	See Knowledge Article: 000038850 on MyVarian		12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Varian	SmartConnect solution Policy Server	All	Affected		Varian Advisory Link	See Knowledge Articles: 000038831 and 000038832 on MyVarian		12/22/2021
Varian	PaaS	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	TrueBeam radiotherapy system	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	UNIQUE system	All	Under Investigation		Varian Advisory Link			12/22/2021
Varian	Varian Authentication and Identity Server (VAIS)	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	Varian Managed Services Cloud	All	Under Investigation		Varian Advisory Link			12/22/2021
Varian	Varian Mobile App	2.0, 2.5	Not Affected		Varian Advisory Link			12/22/2021
Varian	VariSeed	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	Velocity	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	VitalBeam radiotherapy system	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	Vitesse	All	Not Affected		Varian Advisory Link			12/22/2021
Varnish Software					Varnish Software Security Notice			
Varonis					Varonis Notice			
Veeam					Veeam Statement			
Venafi					Venafi Statement			
Veritas NetBackup					Verita Statement			
Vertica					Vertica Statement			
Viso Trust					Viso Trust Statement			
VMware	API Portal for VMware Tanzu	1.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	App Metrics	2.x	Affected	Yes	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	Healthwatch for Tanzu Application Service	2.x, 1.x	Affected	Yes	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	Single Sign-On for VMware Tanzu Application Service	1.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	Spring Cloud Gateway for Kubernetes	1.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	Spring Cloud Gateway for VMware Tanzu	1.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	Spring Cloud Services for VMware Tanzu	3.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	VMware Carbon Black Cloud Workload Appliance	1.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	VMware Carbon Black EDR Server	7.x, 6.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	VMware Cloud Foundation	4.x, 3.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
VMware	VMware HCX	4.x, 3.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	VMware Horizon	8.x, 7.x	Affected	Yes	VMSA-2021-0028.4 (vmware.com)		VMware KB 87073 (vmware.com)	12/17/2021
VMware	VMware Horizon Cloud Connector	1.x, 2.x	Affected	Yes	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	VMware Horizon DaaS	9.1.x, 9.0.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	VMware Identity Manager	3.3.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	VMware NSX-T Data Centern	3.x, 2.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	VMware Site Recovery Manager	8.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	VMware Tanzu Application Service for VMs	2.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	VMware Tanzu GemFire	9.x, 8.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	VMware Tanzu Greenplum	6.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	VMware Tanzu Kubernetes Grid Integrated Edition	1.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	VMware Tanzu Observability by Wavefront Nozzle	3.x, 2.x	Affected	Yes	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	VMware Tanzu Operations Manager	2.x	Affected	Yes	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	VMware Tanzu SQL with MySQL for VMs	2.x, 1.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	VMware Telco Cloud Automation	2.x, 1.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	VMware Unified Access Gateway	21.x, 20.x, 3.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	VMware vCenter Cloud Gateway	1.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	vCenter Server - OVA	7.x, 6.7.x, 6.5.x	Affected	Pending	VMSA-2021-0028.4 (vmware.com)	Workaround @ KB87081 (vmware.com)		2021-12-17
VMware	vCenter Server - Windows	6.7.x, 6.5.x	Affected	Pending	VMSA-2021-0028.4 (vmware.com)	Workaround @ KB87096 (vmware.com)		2021-12-17
VMware	VMware vRealize Automation	8.x, 7.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	VMware vRealize Lifecycle Manager	8.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	VMware vRealize Log Insight	8.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	VMware vRealize Operations	8.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
VMware	VMware vRealize Operations Cloud Proxy	Any	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	VMware vRealize Orchestrator	8.x, 7.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	VMware Workspace ONE Access	21.x, 20.10.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	VMware Workspace ONE Access Connector (VMware Identity Manager Connector)	21.x, 20.10.x, 19.03.0.1	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
Vyaire			Not Affected		Vyaire Advisory Link			12/22/2021
WAGO	WAGO Smart Script	4.2.x < 4.8.1.3	Affected	Yes	WAGO Website			12/17/2021
Wallarm					Lab Mitigation Update			
Wasp Barcode technologies					Waspbarcode Assetcloud Inventorycloud			
WatchGuard	Secplicity				Secplicity Critical RCE			
Western Digital					Westerndigital Product Security			
WIBU Systems	CodeMeter Keyring for TIA Portal	1.30 and prior	Affected	Yes	WIBU Systems Advisory Link	Only the Password Manager is affected		12/22/2021
WIBU Systems	CodeMeter Cloud Lite	2.2 and prior	Affected	Yes	WIBU Systems Advisory Link			12/22/2021
WindRiver					Windriver Security Notice			
WireShark					Gitlab Wireshark			
Wistia					Wistia Incidents			
WitFoo					Witfoo Emergency Update			
WordPress					Wordpress Support			
Worksphere					Workspace Security Update			
Wowza					Wowza Known Issues with Streaming Engine			
WSO2	WSO2 Enterprise Integrator	6.1.0 and above	Affected	Yes	https://docs.wso2.com/pages/viewpage.action?pageId=180948677	A temporary mitigation is available while vendor works on update		
XCP-ng					XCP lOG4j Vulnerability			
XenForo					Xenforo PSA Elasticsearch			
Xerox					Xerox Special Bulletin CVE-2021-44228			
XPertDoc					Xpertdoc			
XPLG					XPLG Secure Log4j			
XWIKI					Xwiki CVE-2021-44228			
Xylem	Aquatalk		Affected	Pacthing complete	Xylem Advisory Link			12/22/2021
Xylem	Avensor		Affected	Pacthing complete	Xylem Advisory Link			12/22/2021
Xylem	Sensus Analytics		Affected	Pacthing complete	Xylem Advisory Link			12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Xylem	Sensus Automation Control Configuration change complete		Affected	Pacthing complete	Xylem Advisory Link			12/22/2021
Xylem	Sensus Cathodic Protection Mitigation in process Mitigation in process		Affected	Mitigation in process	Xylem Advisory Link			12/22/2021
Xylem	Sensus FieldLogic LogServer		Affected	Patching complete	Xylem Advisory Link			12/22/2021
Xylem	Sensus Lighting Control		Affected	Pacthing complete	Xylem Advisory Link			12/22/2021
Xylem	Sensus NetMetrics Configuration change complete		Affected	Pacthing complete	Xylem Advisory Link			12/22/2021
Xylem	Sensus RNI Saas	4.7 through 4.10, 4.4 through 4.6, 4.2	Affected	Pacthing complete	Xylem Advisory Link			12/22/2021
Xylem	Sensus RNI On Prem	4.7 through 4.10, 4.4 through 4.6, 4.2	Affected	Mitigation in process	Xylem Advisory Link			12/22/2021
Xylem	Sensus SCS		Affected	Pacthing complete	Xylem Advisory Link			12/22/2021
Xylem	Smart Irrigation		Affected	Remediation in process	Xylem Advisory Link			12/22/2021
Xylem	Water Loss Management (Visenti)		Affected	Pacthing complete	Xylem Advisory Link			12/22/2021
Xylem	Configuration change complete		Affected	Pacthing complete	Xylem Advisory Link			12/22/2021
Xylem	Xylem Cloud		Affected	Pacthing complete	Xylem Advisory Link			12/22/2021
Xylem	Xylem Edge Gateway (xGW)		Affected	Pacthing complete	Xylem Advisory Link			12/22/2021
Yellowbrick					YellowBrick Security Advisory Yellowbrick			
YellowFin					YellowFinbi Notice Critical Vulnerability in Log4j			
YOKOGAWA			Under Investigation		YOKOGAWA Advisory Link			12/22/2021
YSoft SAFEQ					Ysoft Safeq			
Zabbix					Zabbix Log4j			
ZAMMAD					Zammad Elasticsearch Users			
Zaproxy					Zaproxy			
Zebra					Zebra lifeguard Security			
Zendesk	All Products	All Versions	Affected	No	2021-12-13 Security Advisory - Apache Log4j (CVE-2021-44228)	Zendesk products are all cloud-based; thus there are no updates for the customers to install as the company is working on patching their infrastructure and systems.		12/13/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Zenoss					Zenoss			
Zentera Systems, Inc.	CoIP Access Platform	All	Not Affected		[CVE-2021-44228] Log4Shell Vulnerability in Apache Log4j			12/17/2021
Zerto					Zerto KB			
Zesty					Zesty Log4j Exploit			
Zimbra					BugZilla Zimbra			
Zoom					Zoom Security Exposure			
ZPE systems Inc					ZpeSystems CVE-2021-44228			
Zscaler	See Link (Multiple Products)		Not Affected	No	CVE-2021-44228 log4j Vulnerability			12/15/2021
Zyxel					Zyxel Security Advisory for Apache Log4j			
Zyxel	Security Firewall/Gateways	ZLD Firmware Security Services, Nebula	Not Affected	N/A	Zyxel Security Advisory			12/14/2021