

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

NOTE: This file is automatically generated. To submit updates, please refer to CONTRIBUTING.md.

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
1Password	All products			Not Affected	link			cisagov	2021-01-14
2n				Unknown	link			cisagov	2022-01-12
3CX				Unknown	link			cisagov	2022-01-12
3M Health Information Systems	CGS			Unknown	link	This advisory is available to customer only and has not been reviewed by CISA.		cisagov	2021-12-15
7-Zip				Unknown	link			cisagov	2022-01-12
ABB				Unknown	link			cisagov	2022-01-12
ABB	ABB Remote Service	ABB Remote Platform (RAP)		Affected				cisagov	2022-01-12
ABB	AlarmInsight Cloud	AlarmInsight KPI Dashboards 1.0.0		Affected				cisagov	2022-01-12
ABB	B&R Products	See Vendor Advisory		Affected	link			cisagov	2022-01-12
Abbott				Unknown	link			cisagov	2021-12-15
Abnormal Security	Abnormal Security			Unknown	link			cisagov	2022-01-12
Accellence				Unknown	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Accellion	Kiteworks		v7.6 release	Fixed	link	<p>“As a pre-caution, 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.”</p>		cisagov	2021-12-16
Acquia				Unknown	link			cisagov	2022-01-12
Acronis				Unknown	link			cisagov	2022-01-12
ActiveState				Unknown	link			cisagov	2022-01-12
Adaptec				Unknown	link			cisagov	2022-01-12
Addigy				Unknown	link			cisagov	2022-01-12
Adeptia				Unknown	link			cisagov	2022-01-12
Adobe				Unknown	link			cisagov	2022-01-12
ColdFusion									
ADP				Unknown	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Advanced Systems Concepts (formally Jscape)	Active MFT			Unknown	link	This advisory is available to customers only and has not been reviewed by CISA		cisagov	2021-12-14
Advanced Systems Concepts (formally Jscape)	MFT			Unknown	link	This advisory is available to customers only and has not been reviewed by CISA		cisagov	2021-12-14
Advanced Systems Concepts (formally Jscape)	MFT Gateway			Unknown	link	This advisory is available to customers only and has not been reviewed by CISA		cisagov	2021-12-14
Advanced Systems Concepts (formally Jscape)	MFT Server			Unknown	link	This advisory is available to customers only and has not been reviewed by CISA		cisagov	2021-12-14
AFAS Software				Unknown	link			cisagov	2022-01-12
AFHCAN Global LLC	AFHCANcart			Not Affected	link			cisagov	2022-01-12
AFHCAN Global LLC	AFHCANmobile			Not Affected	link			cisagov	2022-01-12
AFHCAN Global LLC	AFHCANServer			Not Affected	link			cisagov	2022-01-12
AFHCAN Global LLC	AFHCANsuite			Not Affected	link			cisagov	2022-01-12
AFHCAN Global LLC	AFHCANupdate			Not Affected	link			cisagov	2022-01-12
AFHCAN Global LLC	AFHCANweb			Not Affected	link			cisagov	2022-01-12
Agilysys				Unknown	link			cisagov	2022-01-12
Akamai	SIEM Splunk Connector	All		Affected	link	v1.4.11 is the new recommendation for mitigation of log4j vulnerabilities		cisagov	2021-12-15

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Alcatel				Unknown	link			cisagov	2022-01-12
Alertus				Unknown	link			cisagov	2022-01-12
Alexion				Unknown	link			cisagov	2022-01-12
Alfresco				Unknown	link			cisagov	2022-01-12
AlienVault				Unknown	link			cisagov	2022-01-12
Alphatron				Unknown	link			cisagov	2022-01-12
Medical									
Amazon	Athena			Unknown	link			cisagov	2022-01-12
Amazon	AWS			Not Affected		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		cisagov	2021-12-15
Amazon	AWS API Gateway		All	Fixed	link			cisagov	2021-12-20
Amazon	AWS CloudHSM	< 3.4.1.		Affected	link			cisagov	2022-01-12
Amazon	AWS Connect		All	Fixed	link	Vendors recommend evaluating components of the environment outside of the Amazon Connect service boundary, which may require separate/additional customer mitigation		cisagov	2021-12-23
Amazon	AWS DynamoDB		Unknown	Fixed	link			cisagov	2021-12-17

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Amazon	AWS EKS, ECS, Fargate	Unknown		Affected	<a href="#">link</a>	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		cisagov	2021-12-16

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Amazon	AWS ElastiCache		Unknown	Fixed	link			cisagov	2021-12-17
Amazon	AWS ELB		Unknown	Fixed	link			cisagov	2021-12-16
Amazon	AWS Inspector		Unknown	Fixed	link			cisagov	2021-12-17
Amazon	AWS Kinesis Data Stream	Unknown		Affected	link	We are actively patching all sub-systems 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)		cisagov	2021-12-14
Amazon	AWS Lambda	Unknown		Affected	link			cisagov	2022-01-12
Amazon	AWS Lambda	Unknown		Affected	link			cisagov	2022-01-12
Amazon	AWS RDS		Unknown	Fixed	link	Amazon RDS and Amazon Aurora have been updated to mitigate the issues identified in CVE-2021-44228		cisagov	2021-12-17
Amazon	AWS S3		Unknown	Fixed	link			cisagov	2021-12-14

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Amazon	AWS SNS		Unknown	Fixed	link	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		cisagov	2021-12-14
Amazon	AWS SQS		Unknown	Fixed	link			cisagov	2021-12-15
Amazon	CloudFront			Unknown	link			cisagov	2022-01-12
Amazon	CloudWatch			Unknown	link			cisagov	2022-01-12
Amazon	EC2			Not Affected	link			cisagov	2021-12-15
Amazon	ELB			Unknown	link			cisagov	2022-01-12
Amazon	KMS			Unknown	link			cisagov	2022-01-12
Amazon	OpenSearch	Unknown		Affected	link			cisagov	2022-01-12
Amazon	RDS			Unknown	link			cisagov	2022-01-12
Amazon	Route 53			Unknown	link			cisagov	2022-01-12
Amazon	S3			Unknown	link			cisagov	2022-01-12
Amazon	Translate			Unknown	link	Service not identified on AWS Log4j Security Bulletin		cisagov	2022-01-12
Amazon	VPC			Unknown	link			cisagov	2022-01-12
AMD	All			Unknown	link	Currently, no AMD products have been identified as affected. AMD is continuing its analysis.		cisagov	2021-12-22
Anaconda	Anaconda			Not Affected	link			cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Apache	ActiveMQ Artemis			Not Affected	link	ActiveMQ Artemis does not use Log4j for logging. However, Log4j 1.2.17 is included in the Hawtio- based web console ap- plication 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 ap- plication archive. See ARTEMIS- 3612 for more infor- mation on that task.		cisagov	2021-12-21
Apache	Airflow			Unknown	link	Airflow is written in Python		cisagov	2022-01-12



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Apache	Camel	3.14.1.3.11.5, 3.7.7		Affected	link	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.		cisagov	2021-12-13
Apache	Camel 2	<=3.1.4		Unknown	link	The Karaf team is aware of this and are working on a new Karaf 4.3.4 release with updated log4j.		cisagov	2021-12-13
Apache	Camel JBang			Affected	link			cisagov	2021-12-13
Apache	Camel K			Unknown	link			cisagov	2021-12-13
Apache	Camel Karaf			Unknown	link			cisagov	2021-12-13
Apache	Camel Quarkus	< druid 0.22.0		Unknown	link			cisagov	2021-12-13
Apache	CamelKafka Connector			Unknown	link			cisagov	2021-12-13
Apache	Druid			Affected	link			cisagov	2021-12-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Apache	Flink		< 1.14.2, 1.13.5, 1.12.7, 1.11.6	Fixed	link	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	cisagov	2021-12-12
Apache	Kafka			Not Affected	link	The current DB lists Apache Kafka as impacted. Apache Kafka uses Log4jv1, not v2.		cisagov	2021-12-14
Apache	Kafka	Unknown		Affected	link	Only vulnerable in certain configuration(s)		cisagov	2022-01-12
Apache	Log4j	< 2.15.0		Affected	link			cisagov	2022-01-12
Apache	Solr		7.4.0 to 7.7.3, 8.0.0 to 8.11.0	Fixed	link	Update to 8.11.1 or apply fixes as described in Solr security advisory	Apache Solr 8.11.1 downloads	cisagov	2021-12-16

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Apache	Struts 2	Versions before 2.5.28.1		Affected	link	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	cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Apache	Tomcat	9.0.x		Affected	<a href="#">link</a>	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		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
APC by Schneider Electric	Powerchute Business Edition		v9.5, v10.0.1, v10.0.2, v10.0.3, v10.0.4	Fixed	link	Mitigation instructions to remove the affected class.		cisagov	2021-12-15
APC by Schneider Electric	Powerchute Network Shutdown		4.2, 4.3, 4.4, 4.4.1	Fixed	link	Mitigation instructions to remove the affected class.		cisagov	2021-12-15
Apereo	CAS	6.3.x & 6.4.x		Affected	link			cisagov	2022-01-12
Apereo	Opencast	< 9.10, < 10.6		Affected	link			cisagov	2022-01-12
Apigee				Unknown	link			cisagov	2022-01-12
Apollo				Unknown	link			cisagov	2022-01-12
Appdynamics				Unknown	link			cisagov	2022-01-12
Appeon	PowerBuilder	Appeon PowerBuilder 2017-2021 regardless of product edition		Affected				cisagov	2021-12-15
AppGate				Unknown	link			cisagov	2022-01-12
Appian	Appian Platform		All	Fixed	link			cisagov	2021-12-22
Application Performance Ltd	DBMarlin	Not Affected		Affected				cisagov	2021-12-15
Application Performance Ltd	DBMarlin			Unknown	link			cisagov	2021-12-15
APPSHEET				Unknown	link			cisagov	2022-01-12
Aptible	Aptible	ElasticSearch 5.x		Affected	link			cisagov	2022-01-12
Aqua Security				Unknown	link			cisagov	2022-01-12
Arbiter Systems	All			Unknown	link			cisagov	2021-12-22
ARC Informatique	All			Not Affected	link			cisagov	2022-01-13
Arca Noae				Unknown	link			cisagov	2022-01-12
Arcserve	Arcserve Backup			Not Affected	link		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	cisagov	2021-12-14

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Arcserve	Arcserve Continuous Availability			Not Affected	link		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	cisagov	2021-12-14
Arcserve	Arcserve Email Archiving			Not Affected	link		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	cisagov	2021-12-14
Arcserve	Arcserve UDP			Not Affected	link		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	cisagov	2021-12-14

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Arcserve	ShadowProtect			Not Affected	link		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	cisagov	2021-12-14
Arcserve	ShadowXafe			Not Affected	link		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	cisagov	2021-12-14
Arcserve	Solo			Not Affected	link		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	cisagov	2021-12-14

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Arcserve	StorageCraft OneXafe			Not Affected	link		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	cisagov	2021-12-14
ArcticWolf				Unknown	link			cisagov	2022-01-12
Arduino				Unknown	link			cisagov	2022-01-12
Ariba				Unknown	link			cisagov	2022-01-12
Arista				Unknown	link			cisagov	2022-01-12
Aruba Networks				Unknown	link			cisagov	2022-01-12
Ataccama				Unknown	link			cisagov	2022-01-12
Atera				Unknown	link			cisagov	2022-01-12
Atlassian	Bamboo Server & Data Center			Not Affected	link	This product may be affected by a related but lower severity vulnerability if running in a specific non-default configuration.		cisagov	2022-01-12
Atlassian	Bitbucket Server & Data Center	All		Affected	link	This product is not vulnerable to remote code execution but may leak information due to the bundled Elastic-search component being vulnerable.		cisagov	2022-01-12



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Atlassian	Confluence Server & Data Center			Not Affected	link	This product may be affected by a related but lower severity vulnerability if running in a specific non-default configuration.		cisagov	2022-01-12
Atlassian	Crowd Server & Data Center			Not Affected	link	This product may be affected by a related but lower severity vulnerability if running in a specific non-default configuration.		cisagov	2022-01-12
Atlassian	Crucible			Not Affected	link	This product may be affected by a related but lower severity vulnerability if running in a specific non-default configuration.		cisagov	2022-01-12
Atlassian	Fisheye			Not Affected	link	This product may be affected by a related but lower severity vulnerability if running in a specific non-default configuration.		cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Atlassian	Jira Server & Data Center			Not Affected	<a href="#">link</a>	This product may be affected by a related but lower severity vulnerability if running in a specific non-default configuration.		cisagov	2022-01-12
Attivo networks				Unknown	<a href="#">link</a>			cisagov	2022-01-12
Atvise	All			Not Affected	<a href="#">link</a>	The security vulnerability does NOT affect our applications and products or pose any threat. This applies to all Bachmann applications and products, including atvise solutions.		cisagov	2022-01-17
AudioCodes				Unknown	<a href="#">link</a>			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Autodesk				Unknown	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.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Automox				Unknown	link			cisagov	2022-01-12
Autopsy				Unknown	link			cisagov	2022-01-12
Auvik				Unknown	link			cisagov	2022-01-12
Avantra				Unknown	link			cisagov	2022-01-12
SYSLINK									
Avaya	Avaya Analytics	3.5, 3.6, 3.6.1, 3.7, 4		Affected	link			cisagov	2021-12-14
Avaya	Avaya Aura for OneCloud Private			Unknown	link	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.		cisagov	2021-12-14
Avaya	Avaya Aura® Application Enablement Services	8.1.3.2, 8.1.3.3, 10.1		Affected	link		PSN020551u	cisagov	2021-12-14
Avaya	Avaya Aura® Contact Center	7.0.2, 7.0.3, 7.1, 7.1.1, 7.1.2		Affected	link			cisagov	2021-12-14
Avaya	Avaya Aura® Device Services	8, 8.1, 8.1.4, 8.1.5		Affected	link			cisagov	2021-12-14
Avaya	Avaya Aura® Device Services	8.0.1, 8.0.2, 8.1.3		Affected	link			cisagov	2021-12-14
Avaya	Avaya Aura® Media Server	8.0.0, 8.0.1, 8.0.2		Affected	link		PSN020549u	cisagov	2021-12-14
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	link			cisagov	2021-12-14
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	link		PSN020550u	cisagov	2021-12-14
Avaya	Avaya Aura® System Manager	10.1, 8.1.3		Affected	link		PSN005565u	cisagov	2021-12-14
Avaya	Avaya Aura® Web Gateway	3.11[P], 3.8.1[P], 3.8[P], 3.9.1 [P], 3.9[P]		Affected	link			cisagov	2021-12-14
Avaya	Avaya Breeze™	3.7, 3.8, 3.8.1		Affected	link			cisagov	2021-12-14
Avaya	Avaya Contact Center Select	7.0.2, 7.0.3, 7.1, 7.1.1, 7.1.2		Affected	link			cisagov	2021-12-14

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Avaya	Avaya CRM Connector - Connected Desktop	2.2		Affected	link			cisagov	2021-12-14
Avaya	Avaya Device Enablement Service	3.1.22		Affected	link			cisagov	2021-12-14
Avaya	Avaya Meetings	9.1.10, 9.1.11, 9.1.12		Affected	link			cisagov	2021-12-14
Avaya	Avaya one cloud private -UCaaS - Mid Market Aura	1		Affected	link			cisagov	2021-12-14
Avaya	Avaya OneCloud-Private	2		Affected	link			cisagov	2021-12-14
Avaya	Avaya Session Border Controller for Enterprise	8.0.1, 8.1, 8.1.1, 8.1.2, 8.1.3		Affected	link		PSN020554u	cisagov	2021-12-14
Avaya	Avaya Social Media Hub			Unknown	link			cisagov	2021-12-14
Avaya	Avaya Workforce Engagement	5.3		Affected	link			cisagov	2021-12-14
Avaya	Avaya Business Rules Engine	3.4, 3.5, 3.6, 3.7		Affected	link			cisagov	2021-12-14
Avaya	Avaya Callback Assist	5, 5.0.1		Affected	link			cisagov	2021-12-14
Avaya	Avaya Control Manager	9.0.2, 9.0.2.1		Affected	link			cisagov	2021-12-14
Avaya	Avaya Device Enrollment Service	3.1		Affected	link			cisagov	2021-12-14
Avaya	Avaya Equinox™ Conferencing	9.1.2		Affected	link			cisagov	2021-12-14
Avaya	Avaya Interaction Center	7.3.9		Affected	link			cisagov	2021-12-14
Avaya	Avaya IP Office™ Platform	11.0.4, 11.1, 11.1.1, 11.1.2		Affected	link			cisagov	2021-12-14
Avaya	Avaya Proactive Outreach Manager	3.1.2, 3.1.3, 4, 4.0.1		Affected	link			cisagov	2021-12-14
AVEPOINT				Unknown	link			cisagov	2022-01-12
AVM				Unknown	link			cisagov	2022-01-12
AvTech				Unknown	link			cisagov	2022-01-12
RoomAlert									
AWS New				Unknown	link			cisagov	2022-01-12
AXON				Unknown	link			cisagov	2022-01-12
AXS				Unknown	link			cisagov	2022-01-12
Guard									
Axways				Unknown	link			cisagov	2022-01-12
Applications									
B&R	APROL			Unknown	link			cisagov	2021-12-16
Industrial Automation									
BackBox				Unknown	link			cisagov	2022-01-12
Balbix				Unknown	link			cisagov	2022-01-12
Baramundi				Unknown	link			cisagov	2022-01-12
Products									
Barco				Unknown	link			cisagov	2022-01-12
Barracuda				Unknown	link			cisagov	2022-01-12
Baxter				Unknown	link			cisagov	2021-12-20
BBraun	APEX® Compounder			Unknown	link			cisagov	2021-12-20

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
BBraun	DoseTrac® Server, DoseLink™ Server, and Space® Online Suite Server software			Unknown	link			cisagov	2021-12-20
BBraun	Outlook® Safety Infusion System Pump family			Unknown	link			cisagov	2021-12-20
BBraun	Pinnacle® Compounder			Unknown	link			cisagov	2021-12-20
BBraun	Pump, SpaceStation, and Space® Wireless Battery)			Unknown	link			cisagov	2021-12-20
BBraun	Space® Infusion Pump family (Infusomat® Space® Infusion Pump, Perfusor® Space® Infusion			Unknown	link			cisagov	2021-12-20
BD	Arctic Sun™ Analytics			Unknown	link			cisagov	2021-12-20
BD	BD Diabetes Care App Cloud			Unknown	link			cisagov	2021-12-20
BD	BD Health- Sight™ Clinical Advisor			Unknown	link			cisagov	2021-12-20
BD	BD Health- Sight™ Data Manager			Unknown	link			cisagov	2021-12-20
BD	BD Health- Sight™ Diversion Management			Unknown	link			cisagov	2021-12-20
BD	BD Health- Sight™ Infection Advisor			Unknown	link			cisagov	2021-12-20
BD	BD Health- Sight™ Inventory Optimization Analytics			Unknown	link			cisagov	2021-12-20
BD	BD Health- Sight™ Medication Safety			Unknown	link			cisagov	2021-12-20
BD	BD Knowledge Portal for BD Pyxis™ Supply			Unknown	link			cisagov	2021-12-20

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
BD	BD Knowledge Portal for Infusion Technologies			Unknown	link			cisagov	2021-12-20
BD	BD Knowledge Portal for Medication Technologies			Unknown	link			cisagov	2021-12-20
BD	BD Synapsys™ Informatics Solution			Unknown	link			cisagov	2021-12-20
BD	BD Veritor™ COVID At Home Solution Cloud			Unknown	link			cisagov	2021-12-20
Beckman Coulter				Unknown	link			cisagov	2021-12-20
Beijer Electronics	acirro+			Unknown	link			cisagov	2021-12-22
Beijer Electronics	BFI frequency inverters			Unknown	link			cisagov	2021-12-22
Beijer Electronics	BSD servo drives			Unknown	link			cisagov	2021-12-22
Beijer Electronics	CloudVPN			Unknown	link			cisagov	2021-12-22
Beijer Electronics	FnIO-G and M Distributed IO			Unknown	link			cisagov	2021-12-22
Beijer Electronics	iX Developer			Unknown	link			cisagov	2021-12-22
Beijer Electronics	Nexto modular PLC			Unknown	link			cisagov	2021-12-22
Beijer Electronics	Nexto Xpress compact controller			Unknown	link			cisagov	2021-12-22
Beijer Electronics	WARP Engineering Studio			Unknown	link			cisagov	2021-12-22
Bender Best Practical Request Tracker (RT) and Request Tracker for Incident Response (RTIR)				Unknown Unknown	link link			cisagov cisagov	2022-01-12 2022-01-12
BeyondTrust Bomgar				Unknown	link			cisagov	2022-01-12
BeyondTrust	Privilege Management Cloud		Unknown	Fixed	link			cisagov	2021-12-17
BeyondTrust	Privilege Management Reporting in BeyondInsight		21.2	Fixed	link			cisagov	2021-12-17
BeyondTrust	Secure Remote Access appliances			Not Affected	link			cisagov	2021-12-17

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
BioMerieux				Unknown	link			cisagov	2021-12-22
BisectHosting				Unknown	link			cisagov	2022-01-12
BitDefender				Unknown	link			cisagov	2022-01-12
BitNami				Unknown	link			cisagov	2022-01-12
ByVMware									
BitRise				Unknown	link			cisagov	2022-01-12
Bitwarden				Unknown	link			cisagov	2022-01-12
Biztory	Fivetran			Unknown	link		Vendor review indicated Fivetran is not vulnerable to Log4j2	cisagov	2022-01-12
Black Kite				Unknown	link			cisagov	2022-01-12
Blanco				Unknown	link			cisagov	2022-01-12
Blumira				Unknown	link			cisagov	2022-01-12
BMC	Bladelogic Database Automation			Unknown	link			cisagov	2022-01-12
BMC	BMC AMI Ops			Unknown	link			cisagov	2022-01-12
BMC	BMC AMI Products			Unknown	link			cisagov	2022-01-12
BMC	BMC Compuware			Unknown	link			cisagov	2022-01-12
BMC	BMC Helix Automation Console			Unknown	link			cisagov	2022-01-12
BMC	BMC Helix Business Workflows			Unknown	link			cisagov	2022-01-12
BMC	BMC Helix Client Management			Unknown	link			cisagov	2022-01-12
BMC	BMC Helix Cloud Cost			Unknown	link			cisagov	2022-01-12
BMC	BMC Helix Cloud Security			Unknown	link			cisagov	2022-01-12
BMC	BMC Helix CMDB			Unknown	link			cisagov	2022-01-12
BMC	BMC Helix Continuous Optimization			Unknown	link			cisagov	2022-01-12
BMC	BMC Helix Control-M			Unknown	link			cisagov	2022-01-12
BMC	BMC Helix Digital Workplace			Unknown	link			cisagov	2022-01-12
BMC	BMC Helix Discovery			Unknown	link			cisagov	2022-01-12
BMC	BMC Helix ITSM			Unknown	link			cisagov	2022-01-12
BMC	BMC Helix Knowledge Management			Unknown	link			cisagov	2022-01-12
BMC	BMC Helix Operations Management with AIOps			Unknown	link			cisagov	2022-01-12
BMC	BMC Helix Platform			Unknown	link			cisagov	2022-01-12
BMC	BMC Helix platform			Unknown	link			cisagov	2022-01-12
BMC	BMC Helix Remediate			Unknown	link			cisagov	2022-01-12
BMC	BMC Helix Remediate			Unknown	link			cisagov	2022-01-12



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
BMC	BMC Helix			Unknown	link			cisagov	2022-01-12
BMC	Remedyforce			Unknown	link			cisagov	2022-01-12
BMC	BMC Helix Virtual Agent			Unknown	link			cisagov	2022-01-12
BMC	Cloud Lifecycle Management			Unknown	link			cisagov	2022-01-12
BMC	Control-M			Unknown	link			cisagov	2022-01-12
BMC	Footprints			Unknown	link			cisagov	2022-01-12
BMC	MainView			Unknown	link			cisagov	2022-01-12
BMC	Middleware Administrator			Unknown	link			cisagov	2022-01-12
BMC	MainView Middleware Monitor			Unknown	link			cisagov	2022-01-12
BMC	Remedy ITSM (IT Service Management)			Unknown	link			cisagov	2022-01-12
BMC	SmartIT			Unknown	link			cisagov	2022-01-12
BMC	Track-It!			Unknown	link			cisagov	2022-01-12
BMC	TrueSight			Unknown	link			cisagov	2022-01-12
BMC	Automation for Networks			Unknown	link			cisagov	2022-01-12
BMC	TrueSight Automation for Servers			Unknown	link			cisagov	2022-01-12
BMC	TrueSight Capacity Optimization			Unknown	link			cisagov	2022-01-12
BMC	TrueSight In-frastructure Management			Unknown	link			cisagov	2022-01-12
BMC	TrueSight Operations Management			Unknown	link			cisagov	2022-01-12
BMC	TrueSight Orchestration			Unknown	link			cisagov	2022-01-12
Bosch				Unknown	link			cisagov	2021-12-22
Boston Scientific				Unknown	link			cisagov	2021-12-20
Box				Unknown	link			cisagov	2022-01-12
Brainworks				Unknown	link			cisagov	2022-01-12
BrightSign				Unknown	link			cisagov	2022-01-12
Broadcom	Advanced Secure Gateway (ASG)			Unknown	link			cisagov	2022-01-12
Broadcom	Automic Automation			Unknown	link			cisagov	2022-01-12
Broadcom	BCAAA			Unknown	link			cisagov	2022-01-12
Broadcom	CA Advanced Authentication	9.1		Affected				cisagov	2022-01-12
Broadcom	CA Risk Authentication			Unknown				cisagov	2022-01-12
Broadcom	CA Strong Authentication			Unknown				cisagov	2022-01-12
Broadcom	Cloud Workload Protection (CWP)			Unknown	link			cisagov	2022-01-12
Broadcom	Cloud Workload Protection for Storage (CWP:S)			Unknown	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Broadcom	CloudSOC Cloud Access Security Broker (CASB)			Unknown	link			cisagov	2022-01-12
Broadcom	Content Analysis (CA)			Unknown	link			cisagov	2022-01-12
Broadcom	Critical System Protection (CSP)			Unknown	link			cisagov	2022-01-12
Broadcom	Data Center Security (DCS)			Unknown	link			cisagov	2022-01-12
Broadcom	Data Loss Prevention (DLP)			Unknown	link			cisagov	2022-01-12
Broadcom	Email Security Service (ESS)			Unknown	link			cisagov	2022-01-12
Broadcom	Ghost Solution Suite (GSS)			Unknown	link			cisagov	2022-01-12
Broadcom	HSM Agent			Unknown	link			cisagov	2022-01-12
Broadcom	Industrial Control System Protection (ICSP)			Unknown	link			cisagov	2022-01-12
Broadcom	Integrated Cyber Defense Manager (ICDm)			Unknown	link			cisagov	2022-01-12
Broadcom	Integrated Secure Gateway (ISG)			Unknown	link			cisagov	2022-01-12
Broadcom	IT Management Suite			Unknown	link			cisagov	2022-01-12
Broadcom	Layer7 API Developer Portal			Unknown	link			cisagov	2022-01-12
Broadcom	Layer7 API Gateway			Unknown	link			cisagov	2022-01-12
Broadcom	Layer7 Mobile API Gateway			Unknown	link			cisagov	2022-01-12
Broadcom	Management Center (MC)			Unknown	link			cisagov	2022-01-12
Broadcom	PacketShaper (PS) S-Series			Unknown	link			cisagov	2022-01-12
Broadcom	PolicyCenter (PC) S-Series			Unknown	link			cisagov	2022-01-12
Broadcom	Privileged Access Manager			Unknown	link			cisagov	2022-01-12
Broadcom	Privileged Access Manager Server Control			Unknown	link			cisagov	2022-01-12
Broadcom	Privileged Identity Manager			Unknown	link			cisagov	2022-01-12
Broadcom	ProxySG			Unknown	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Broadcom	Reporter			Unknown	link			cisagov	2022-01-12
Broadcom	Secure Access Cloud (SAC)			Unknown	link			cisagov	2022-01-12
Broadcom	Security Analytics (SA)			Unknown	link			cisagov	2022-01-12
Broadcom	SiteMinder (CA Single Sign-On)			Unknown	link			cisagov	2022-01-12
Broadcom	SSL Visibility (SSLV)			Unknown	link			cisagov	2022-01-12
Broadcom	Symantec Control Compliance Suite (CCS)			Unknown	link			cisagov	2022-01-12
Broadcom	Symantec Directory			Unknown	link			cisagov	2022-01-12
Broadcom	Symantec Endpoint Detection and Response (EDR)			Unknown	link			cisagov	2022-01-12
Broadcom	Symantec Endpoint Encryption (SEE)			Unknown	link			cisagov	2022-01-12
Broadcom	Symantec Endpoint Protection (SEP)			Unknown	link			cisagov	2022-01-12
Broadcom	Symantec Endpoint Protection (SEP) for Mobile			Unknown	link			cisagov	2022-01-12
Broadcom	Symantec Endpoint Protection Manager (SEPM)	14.3		Affected	link			cisagov	2022-01-12
Broadcom	Symantec Identity Governance and Administration (IGA)			Unknown	link			cisagov	2022-01-12
Broadcom	Symantec Mail Security for Microsoft Exchange (SMSMSE)			Unknown	link			cisagov	2022-01-12
Broadcom	Symantec Messaging Gateway (SMG)			Unknown	link			cisagov	2022-01-12
Broadcom	Symantec PGP Solutions			Unknown	link			cisagov	2022-01-12
Broadcom	Symantec Protection Engine (SPE)			Unknown	link			cisagov	2022-01-12
Broadcom	Symantec Protection for SharePoint Servers (SPSS)			Unknown	link			cisagov	2022-01-12
Broadcom	VIP			Unknown	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Broadcom	VIP Authentication Hub			Unknown	link			cisagov	2022-01-12
Broadcom	Web Isolation (WI)			Unknown	link			cisagov	2022-01-12
Broadcom	Web Security Service (WSS)			Unknown	link			cisagov	2022-01-12
Broadcom C4b	WebPulse			Unknown	link			cisagov	2022-01-12
XPHONE				Unknown	link			cisagov	2022-01-12
Campbell Scientific	All			Unknown	link			cisagov	2021-12-23
Camunda				Unknown	link			cisagov	2022-01-12
Canary Labs	All			Unknown	link			cisagov	2021-12-22
Canon	Alphenix (Angio Workstation)			Unknown	link			cisagov	2021-12-22
Canon	CT Medical Imaging Products			Unknown	link			cisagov	2021-12-22
Canon	Infinix-i (Angio Workstation)			Unknown	link			cisagov	2021-12-22
Canon	MR Medical Imaging Products			Unknown	link			cisagov	2021-12-22
Canon	NM Medical Imaging Products			Unknown	link			cisagov	2021-12-22
Canon	UL Medical Imaging Products			Unknown	link			cisagov	2021-12-22
Canon	Vitrea			Unknown	link			cisagov	2021-12-22
Canon	Advanced 7.x XR Medical Imaging Products			Unknown	link			cisagov	2021-12-22
CapStorm	Copystorm			Unknown				cisagov	2021-12-22
CarbonBlack				Unknown	link			cisagov	2022-01-12
Carestream				Unknown	link			cisagov	2021-12-20
Carrier				Unknown	link			cisagov	2022-01-12
CAS				Unknown	link			cisagov	2022-01-12
genesisWorld				Unknown	link			cisagov	2022-01-12
Cato Networks				Unknown	link			cisagov	2022-01-12
Cepheid	C360			Unknown	link			cisagov	2021-12-20
Cepheid	GeneXpert			Unknown	link			cisagov	2021-12-20
Cerberus				Unknown	link			cisagov	2022-01-12
FTP				Unknown	link			cisagov	2022-01-12
Chaser	discrimiNAT			Not Affected	link			cisagov	2022-01-12
Systems	Firewall			Not Affected	link			cisagov	2022-01-12
Check Point	CloudGuard			Not Affected	link			cisagov	2022-01-12
Check Point	Harmony			Not Affected	link			cisagov	2022-01-12
Check Point	Endpoint & Harmony Mobile			Not Affected	link			cisagov	2022-01-12
Check Point	Infinity Portal			Unknown	link			cisagov	2022-01-12
Check Point	Quantum Security Gateway			Not Affected	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Check Point	Quantum Security Management			Not Affected	link	Where used, uses the 1.8.0_u241 version of the JRE that protects against this attack by default.		cisagov	2022-01-12
Check Point	SMB			Not Affected	link			cisagov	2022-01-12
Check Point	ThreatCloud			Unknown	link			cisagov	2022-01-12
CheckMK				Unknown	link			cisagov	2022-01-12
Ciphermail				Unknown	link			cisagov	2022-01-12
CircleCI	CircleCI			Unknown	link			cisagov	2021-12-21
CIS				Unknown	link			cisagov	2022-01-12
Cisco	AppDynamics			Unknown	link			cisagov	2022-01-12
Cisco	Cisco ACI Multi-Site Orchestrator			Unknown	link			cisagov	2022-01-12
Cisco	Cisco ACI Virtual Edge			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Adaptive Security Appliance (ASA) Software			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Advanced Web Security Reporting Application			Unknown	link			cisagov	2022-01-12
Cisco	Cisco AMP Virtual Private Cloud Appliance			Unknown	link			cisagov	2022-01-12
Cisco	Cisco AnyConnect Secure Mobility Client			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Application Policy Infrastructure Controller (APIC)			Unknown	link			cisagov	2022-01-12
Cisco	Cisco ASR 5000 Series Routers			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Broadcloud Calling			Unknown	link			cisagov	2022-01-12
Cisco	Cisco BroadWorks			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Catalyst 9800 Series Wireless Controllers			Unknown	link			cisagov	2022-01-12
Cisco	Cisco CloudCenter Suite Admin			Unknown	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Cisco	Cisco CloudCenter Workload Manager			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Cognitive Intelligence			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Common Services Platform Collector			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Computer Telephony Integration Object Server (CTIOS)			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Connected Grid Device Manager			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Connected Mobile Experiences			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Connectivity			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Contact Center Domain Manager (CCDM)			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Contact Center Management Portal (CCMP)			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Crosswork Change Automation			Unknown	link			cisagov	2022-01-12
Cisco	Cisco CX Cloud Agent Software			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Data Center Network Manager (DCNM)			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Defense Orchestrator			Unknown	link			cisagov	2022-01-12
Cisco	Cisco DNA Assurance			Unknown	link			cisagov	2022-01-12
Cisco	Cisco DNA Center			Unknown	link			cisagov	2022-01-12
Cisco	Cisco DNA Spaces			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Elastic Services Controller (ESC)			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Emergency Responder			Unknown	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Cisco	Cisco Enterprise Chat and Email			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Enterprise NFV Infrast- ructure Software (NFVIS)			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Evolved Pro- grammable Network Manager			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Extensible Network Controller (XNC)			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Finesse			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Firepower Management Center			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Firepower Threat Defense (FTD)			Unknown	link			cisagov	2022-01-12
Cisco	Cisco GGSN Gateway GPRS Support Node			Unknown	link			cisagov	2022-01-12
Cisco	Cisco HyperFlex System			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Identity Services Engine (ISE)			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Integrated Management Controller (IMC)			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Supervisor			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Intersight			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Intersight Virtual Appliance			Unknown	link			cisagov	2022-01-12
Cisco	Cisco IOS and IOS XE Software			Unknown	link			cisagov	2022-01-12
Cisco	Cisco IoT Field Network Director (formerly Cisco Connected Grid Network Management System)			Unknown	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Cisco	Cisco IoT Operations Dashboard			Unknown	link			cisagov	2022-01-12
Cisco	Cisco IOx Fog Director			Unknown	link			cisagov	2022-01-12
Cisco	Cisco IP Services Gateway (IPSG)			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Kinetic for Cities			Unknown	link			cisagov	2022-01-12
Cisco	Cisco MDS 9000 Series Multilayer Switches			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Meeting Server			Unknown	link			cisagov	2022-01-12
Cisco	Cisco MME Mobility Management Entity			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Modeling Labs			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Network Assessment (CNA) Tool			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Network Assurance Engine			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Network Convergence System 2000 Series			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Network Planner			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Network Services Orchestrator (NSO)			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Nexus 5500 Platform Switches			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Nexus 5600 Platform Switches			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Nexus 6000 Series Switches			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Nexus 7000 Series Switches			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode			Unknown	link			cisagov	2022-01-12



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Cisco	Cisco Nexus Dashboard (formerly Cisco Application Services Engine)			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Nexus Data Broker			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Nexus Insights			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Optical Network Planner			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Packaged Contact Center Enterprise			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Paging Server			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Paging Server (InformaCast)			Unknown	link			cisagov	2022-01-12
Cisco	Cisco PDSN/HA Packet Data Serving Node and Home Agent			Unknown	link			cisagov	2022-01-12
Cisco	Cisco PGW Packet Data Network Gateway			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Policy Suite			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Prime Central for Service Providers			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Prime Collaboration Manager			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Prime Collaboration Provisioning			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Prime Infrastructure			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Prime License Manager			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Prime Network			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Prime Optical for Service Providers			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Prime Provisioning			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Prime Service Catalog			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Registered Envelope Service			Unknown	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Cisco	Cisco SD-WAN vEdge 1000 Series Routers			Unknown	link			cisagov	2022-01-12
Cisco	Cisco SD-WAN vEdge 2000 Series Routers			Unknown	link			cisagov	2022-01-12
Cisco	Cisco SD-WAN vEdge 5000 Series Routers			Unknown	link			cisagov	2022-01-12
Cisco	Cisco SD-WAN vEdge Cloud Router Platform			Unknown	link			cisagov	2022-01-12
Cisco	Cisco SD-WAN vManage			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Secure Network Analytics (SNA), formerly Stealthwatch			Unknown	link			cisagov	2022-01-12
Cisco	Cisco SocialMiner			Unknown	link			cisagov	2022-01-12
Cisco	Cisco System Architecture Evolution Gateway (SAEGW)			Unknown	link			cisagov	2022-01-12
Cisco	Cisco TelePresence Management Suite			Unknown	link			cisagov	2022-01-12
Cisco	Cisco UCS Director			Unknown	link			cisagov	2022-01-12
Cisco	Cisco UCS Performance Manager			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Umbrella			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Unified Attendant Console			Unknown	link			cisagov	2022-01-12
Cisco	Advanced Cisco Unified Attendant Console Business Edition			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Unified Attendant Console Department Edition			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Unified Attendant Console Enterprise Edition			Unknown	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Cisco	Cisco Unified Attendand Console Premium Edition			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Unified Communica- tions Manager Cloud			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Unified Contact Center			Unknown	link			cisagov	2022-01-12
Cisco	Enterprise Cisco Unified Contact Center Enterprise - Live Data server			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Unified Contact Center Express			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Unified Intelligent Contact Management Enterprise			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Unified SIP Proxy Software			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Video Surveillance Operations Manager			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Virtual Topology System - Virtual Topology Controller (VTC) VM			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Virtualized Voice Browser			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Vision Dynamic Signage Director			Unknown	link			cisagov	2022-01-12
Cisco	Cisco WAN Automation Engine (WAE)			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Web Security Appliance (WSA)			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Webex Cloud- Connected UC (CCUC)			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Webex Meetings Server			Unknown	link			cisagov	2022-01-12
Cisco	Cisco Webex Teams			Unknown	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Cisco	Cisco Wide Area Application Services (WAAS)			Unknown	link			cisagov	2022-01-12
Cisco	Duo			Unknown	link			cisagov	2022-01-12
Cisco	DUO network gateway (on-prem/self-hosted)			Unknown				cisagov	2022-01-12
Cisco	duo network gateway (on-prem/self-hosted)			Unknown				cisagov	2022-01-12
Cisco	Exony Virtualized Interaction Manager (VIM)			Unknown	link			cisagov	2022-01-12
Cisco	Managed Services Accelerator (MSX) Network Access Control Service			Unknown	link			cisagov	2022-01-12
Citrix	Citrix ADC (NetScaler ADC) and Citrix Gateway (NetScaler Gateway)			Not Affected	link	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.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Citrix	Citrix Application Delivery Management (NetScaler MAS)			Not Affected	link	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.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Citrix	Citrix Cloud Connector			Unknown	link	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.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Citrix	Citrix Connector Appliance for Cloud Services			Unknown	link	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.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Citrix	Citrix Content Collaboration (ShareFile Integration) – Citrix Files for Windows, Citrix Files for Mac, Citrix Files for Outlook			Unknown	link	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.		cisagov	2021-12-21



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Citrix	Citrix Endpoint Management (Citrix XenMobile Server)			Unknown	link	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.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Citrix	Citrix Hypervisor (XenServer)			Unknown	link	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.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Citrix	Citrix License Server			Unknown	<a href="#">link</a>	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.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Citrix	Citrix SD-WAN			Not Affected	link	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.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Citrix	Citrix Virtual Apps and Desktops (XenApp & XenDesktop)			Unknown	link	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.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Citrix	Citrix Workspace App			Not Affected	link	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.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Citrix	ShareFile Storage Zones Controller			Unknown	link	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.		cisagov	2021-12-21
Claris				Unknown	link			cisagov	2022-01-12
Cloudera	AM2CM Tool			Unknown	link			cisagov	2022-01-12
Cloudera	Ambari	Only versions 2.x, 1.x		Affected	link			cisagov	2022-01-12
Cloudera	Arcadia	Only version 7.1.x		Affected	link			cisagov	2022-01-12
Cloudera	Enterprise CDH, HDP, and HDF	Only version 6.x		Affected	link			cisagov	2022-01-12
Cloudera	CDP Operational Database (COD)			Unknown	link			cisagov	2022-01-12
Cloudera	CDP Private Cloud Base	Only version 7.x		Affected	link			cisagov	2022-01-12
Cloudera	CDS 3 Powered by Apache Spark	All versions		Affected	link			cisagov	2022-01-12
Cloudera	CDS 3.2 for GPUs	All versions		Affected	link			cisagov	2022-01-12
Cloudera	Cloudera Cybersecurity Platform	All versions		Affected	link			cisagov	2022-01-12
Cloudera	Cloudera Data Engineering (CDE)			Unknown	link			cisagov	2022-01-12
Cloudera	Cloudera Data Engineering (CDE)	All versions		Affected	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Cloudera	Cloudera Data Flow (CFM)	Only versions 2.x, 3.x		Unknown	link			cisagov	2022-01-12
Cloudera	Cloudera Data Science Workbench (CDSW)			Affected	link			cisagov	2022-01-12
Cloudera	Cloudera Data Visualization (CDV)			Unknown	link			cisagov	2022-01-12
Cloudera	Cloudera Data Warehouse (CDW)			Unknown	link			cisagov	2022-01-12
Cloudera	Cloudera Data Warehouse (CDW)	All versions		Affected	link			cisagov	2022-01-12
Cloudera	Cloudera DataFlow (CDF)	All versions		Unknown	link			cisagov	2022-01-12
Cloudera	Cloudera Edge Management (CEM)			Affected	link			cisagov	2022-01-12
Cloudera	Cloudera Enterprise			Affected	link			cisagov	2022-01-12
Cloudera	Cloudera Flow Management (CFM)			Unknown	link			cisagov	2022-01-12
Cloudera	Cloudera Machine Learning (CML)	All versions		Affected	link			cisagov	2022-01-12
Cloudera	Cloudera Machine Learning (CML)	All versions		Affected	link			cisagov	2022-01-12
Cloudera	Cloudera Manager (Including Backup Disaster Recovery (BDR) and Replication Manager)								
Cloudera	Cloudera Manager (Including Backup Disaster Recovery (BDR) and Replication Manager)								
Cloudera	Cloudera Manager (Including Backup Disaster Recovery (BDR) and Replication Manager)								
Cloudera	Cloudera Manager (Including Backup Disaster Recovery (BDR) and Replication Manager)	Only versions 7.0.x, 7.1.x, 7.2.x		Affected	link			cisagov	2022-01-12
Cloudera	Cloudera Manager (Including Backup Disaster Recovery (BDR))			Unknown	link			cisagov	2022-01-12



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	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	link			cisagov	2022-01-12
Cloudera	Cloudera Stream Processing (CSP)	All versions		Affected	link			cisagov	2022-01-12
Cloudera	Cloudera Streaming Analytics (CSA)			Unknown	link			cisagov	2022-01-12
Cloudera	Cloudera Streaming Analytics (CSA)			Unknown	link			cisagov	2022-01-12
Cloudera	Data Analytics Studio (DAS)			Unknown	link			cisagov	2022-01-12
Cloudera	Data Catalog			Unknown	link			cisagov	2022-01-12
Cloudera	Data Lifecycle Manager (DLM)			Unknown	link			cisagov	2022-01-12
Cloudera	Data Steward Studio (DSS)	All versions		Affected	link			cisagov	2022-01-12
Cloudera	Hortonworks Data Flow (HDF)			Unknown	link			cisagov	2022-01-12
Cloudera	Hortonworks Data Platform (HDP)	Only versions 7.1.x, 2.7.x, 2.6.x		Affected	link			cisagov	2022-01-12
Cloudera	Hortonworks DataPlane Platform			Unknown	link			cisagov	2022-01-12
Cloudera	Management Console	All versions		Affected	link			cisagov	2022-01-12
Cloudera	Management Console for CDP Public Cloud			Unknown	link			cisagov	2022-01-12
Cloudera	Replication Manager			Unknown	link			cisagov	2022-01-12
Cloudera	SmartSense			Unknown	link			cisagov	2022-01-12
Cloudera	Workload Manager			Unknown	link			cisagov	2022-01-12
Cloudera	Workload XM	All versions		Affected	link			cisagov	2022-01-12
Cloudera	Workload XM (SaaS)			Unknown	link			cisagov	2022-01-12
CloudFlare				Unknown	link			cisagov	2022-01-12
Cloudian	HyperStore			Unknown	link			cisagov	2022-01-12
Cloudogu	Ecosystem	All		Affected	link			cisagov	2022-01-12
Cloudogu	SCM-Manager			Unknown	link			cisagov	2022-01-12
Cloudron				Unknown	link			cisagov	2022-01-12
Clover				Unknown	link			cisagov	2022-01-12
Code42	Code42 App		8.8.1	Fixed	link			cisagov	2021-12-22

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Code42	Crashplan		8.8, possibly prior versions	Fixed	link	I think, they don't specify in the notice, but we know that they released an updated Crashplan client. Possibly prior versions affected.		cisagov	2021-12-16
CodeBeamer				Unknown	link			cisagov	2022-01-12
Codesys				Unknown	link			cisagov	2022-01-12
Cohesity				Unknown	link			cisagov	2022-01-12
CommVault				Unknown	link			cisagov	2022-01-12
Concourse	Concourse			Unknown	link			cisagov	2022-01-12
ConcreteCMS.com				Unknown	link			cisagov	2022-01-12
Confluent	Confluent Cloud		N/A	Fixed	link			cisagov	2021-12-17
Confluent	Confluent ElasticSearch Sink	<11.1.7		Affected	link			cisagov	2021-12-17
Confluent	Confluent Connector for Kubernetes			Not Affected	link			cisagov	2021-12-17
Confluent	Confluent Google DataProc Sink	<1.1.5		Affected	link			cisagov	2021-12-17
Confluent	Confluent HDFS 2 Sink	<10.1.3		Affected	link			cisagov	2021-12-17
Confluent	Confluent HDFS 3 Sink	<1.1.8		Affected	link			cisagov	2021-12-17
Confluent	Confluent Kafka Connectors			Not Affected	link			cisagov	2021-12-17
Confluent	Confluent Platform	<7.0.1		Affected	link			cisagov	2021-12-17
Confluent	Confluent Splunk Sink	<2.05		Affected	link			cisagov	2021-12-17
Confluent	Confluent VMWare Tanzu GemFire Sink	<1.0.8		Affected	link			cisagov	2021-12-17
Connect2id				Unknown	link			cisagov	2022-01-12
ConnectWise				Unknown	link			cisagov	2022-01-12
ContrastSecurity				Unknown	link			cisagov	2022-01-12
ControlUp				Unknown	link			cisagov	2022-01-12
COPADATA All				Unknown	link			cisagov	2022-01-06
CouchBase				Unknown	link			cisagov	2022-01-12
CPanel				Unknown	link			cisagov	2022-01-12
Cradlepoint				Unknown	link			cisagov	2022-01-12
Crestron				Unknown	link			cisagov	2021-12-20
CrushFTP				Unknown	link			cisagov	2022-01-12
CryptShare				Unknown	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
CyberArk	Privileged Threat Analytics (PTA)		N/A	Fixed	link		This advisory is available to customers only and has not been reviewed by CISA.	cisagov	2021-12-14
Cybereason				Unknown	link			cisagov	2022-01-12
CyberRes				Unknown	link			cisagov	2022-01-12
Daktronics	All Sport Pro			Unknown	link			cisagov	2022-01-06
Daktronics	Dakronics Media Player			Not Affected	link			cisagov	2022-01-06
Daktronics	Dakronics Web Player	DWP-1000		Affected	link	DWP-1000: Not present in our codebase, but awaiting confirmation from LG re: webOS platform.		cisagov	2022-01-06
Daktronics	Data Vision Software (DVS)			Unknown	link	DVS has one microservice that uses Log4j, but it uses a version that is not impacted.		cisagov	2022-01-06
Daktronics	Dynamic Messaging System (DMS)			Unknown	link			cisagov	2022-01-06
Daktronics	Dynamic Messaging System - DMS Core Player			Not Affected	link			cisagov	2022-01-06
Daktronics	Dynamic Messaging System - DMS Player hardware			Not Affected	link			cisagov	2022-01-06
Daktronics	Dynamic Messaging System - DMS Web Player			Unknown	link	DMS Web Player: Not present in our codebase, but awaiting confirmation from LG re: webOS platform.		cisagov	2022-01-06
Daktronics	IBoot - Dataprobe IBoot Devices			Not Affected	link			cisagov	2022-01-06
Daktronics	Outdoor Smartlink Devices			Not Affected	link			cisagov	2022-01-06

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Daktronics	Routers - Cisco Meraki Z3/Z3c Routers	A-3350704		Not Affected	link			cisagov	2022-01-06
Daktronics	Routers - Cisco Z1 Routers			Not Affected	link			cisagov	2022-01-06
Daktronics	Routers - Sierra Wireless RV50x/RV50			Affected	link			cisagov	2022-01-06
Daktronics	Show Control System (SCS)			Unknown	link			cisagov	2022-01-06
Daktronics	Vanguard			Unknown	link			cisagov	2022-01-06
Daktronics	Venus 1500			Unknown	link			cisagov	2022-01-06
Daktronics	Venus Control Suite (VCS)			Unknown	link			cisagov	2022-01-06
Daktronics	Video Image Processors			Not Affected	link			cisagov	2022-01-06
Daktronics	Webcam - Mobotix			Not Affected	link			cisagov	2022-01-06
DarkTrace				Unknown	link			cisagov	2022-01-12
Dassault Systèmes				Unknown	link			cisagov	2022-01-12
Databricks				Unknown	link			cisagov	2022-01-12
Datadog	Datadog Agent		>=6.17.0, <=6.32.2, >=7.17.0, <=7.32.2	Fixed	link			cisagov	2022-01-12
Dataminer				Unknown	link			cisagov	2022-01-12
Datev				Unknown	link			cisagov	2022-01-12
Datto				Unknown	link			cisagov	2022-01-12
dCache.org				Unknown	link			cisagov	2022-01-12
Debian				Unknown	link			cisagov	2022-01-12
Deepinstinct				Unknown	link			cisagov	2022-01-12
Dell	“Dell EMC PowerMax VMAX VMAX3 and VMAX AFA”			Not Affected	link			cisagov	2021-12-15
Dell	“Dell EMC PowerSwitch Z9264F-ON BMC Dell EMC PowerSwitch Z9432F-ON BMC”			Not Affected	link			cisagov	2021-12-15
Dell	Alienware Command Center			Not Affected	link			cisagov	2021-12-15
Dell	Alienware OC Controls			Not Affected	link			cisagov	2021-12-15
Dell	Alienware On Screen Display			Not Affected	link			cisagov	2021-12-15
Dell	Alienware Update			Not Affected	link			cisagov	2021-12-15
Dell	APEX Console		N/A	Fixed	link	Cloud environment patched		cisagov	2021-12-15
Dell	APEX Data Storage Services			Unknown	link	Cloud environment patch in progress		cisagov	2021-12-15
Dell	Atmos			Not Affected	link			cisagov	2021-12-15

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Dell	Azure Stack HCI			Not Affected	link			cisagov	2021-12-15
Dell	CalMAN Powered Calibration Firmware			Not Affected	link			cisagov	2021-12-15
Dell	CalMAN Ready for Dell			Not Affected	link			cisagov	2021-12-15
Dell	Centera			Not Affected	link			cisagov	2021-12-15
Dell	Chameleon Linux Based Diagnostics Chassis			Not Affected	link			cisagov	2021-12-15
Dell	Management Controller (CMC)			Not Affected	link			cisagov	2021-12-15
Dell	China HDD Deluxe			Not Affected	link			cisagov	2021-12-15
Dell	Cloud IQ			Unknown	link	Cloud environment patched		cisagov	2021-12-15
Dell	Cloud Mobility for Dell EMC Storage			Not Affected	link			cisagov	2021-12-15
Dell	Cloud Tiering Appliance			Not Affected	link			cisagov	2021-12-15
Dell	Connectrix (Cisco MDS 9000 switches)			Not Affected	link			cisagov	2021-12-15
Dell	Connectrix (Cisco MDS DCNM)			Unknown	link	Patch expected by 12/23/21		cisagov	2021-12-15
Dell	Connectrix B-Series SANnav	2.1.1		Affected	link	Patch expected by 3/31/2022		cisagov	2021-12-15
Dell	Connextrix B Series			Not Affected	link			cisagov	2021-12-15
Dell	CyberSecIQ Application			Not Affected	link			cisagov	2021-12-15
Dell	CyberSense for PowerProtect Cyber Recovery			Not Affected	link			cisagov	2021-12-15
Dell	Data Domain OS	Versions between 7.3.0.5 and 7.7.0.6; Versions before 7.6.0.30		Affected	link	See DSA-2021-274		cisagov	2021-12-15
Dell	Dell BSAFE Crypto-C Micro Edition			Not Affected	link			cisagov	2021-12-15
Dell	Dell BSAFE Crypto-J			Not Affected	link			cisagov	2021-12-15
Dell	Dell BSAFE Micro Edition Suite			Not Affected	link			cisagov	2021-12-15
Dell	Dell Calibration Assistant			Not Affected	link			cisagov	2021-12-15
Dell	Dell Cinema Color			Not Affected	link			cisagov	2021-12-15

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Dell	Dell Cloud Command Repository Manager			Not Affected	link			cisagov	2021-12-15
Dell	Dell Cloud Management Agent			Not Affected	link			cisagov	2021-12-15
Dell	Dell Color Management			Not Affected	link			cisagov	2021-12-15
Dell	Dell Command Configure			Not Affected	link			cisagov	2021-12-15
Dell	Dell Command Integration Suite for System Center			Not Affected	link			cisagov	2021-12-15
Dell	Dell Command Intel vPro Out of Band			Not Affected	link			cisagov	2021-12-15
Dell	Dell Command Monitor			Not Affected	link			cisagov	2021-12-15
Dell	Dell Command Power Manager			Not Affected	link			cisagov	2021-12-15
Dell	Dell Command PowerShell Provider			Not Affected	link			cisagov	2021-12-15
Dell	Dell Command Update			Not Affected	link			cisagov	2021-12-15
Dell	Dell Customer Connect			Not Affected	link			cisagov	2021-12-15
Dell	Dell Data Guardian*			Not Affected	link			cisagov	2021-12-15
Dell	Dell Data Protection*			Not Affected	link			cisagov	2021-12-15
Dell	Dell Data Recovery Environment			Not Affected	link			cisagov	2021-12-15
Dell	Dell Data Vault			Not Affected	link			cisagov	2021-12-15
Dell	Dell Data Vault for Chrome OS			Not Affected	link			cisagov	2021-12-15
Dell	Dell Deployment Agent			Not Affected	link			cisagov	2021-12-15
Dell	Dell Digital Delivery			Not Affected	link			cisagov	2021-12-15
Dell	Dell Direct USB Key			Not Affected	link			cisagov	2021-12-15
Dell	Dell Display Manager 1.5 for Windows / macOS			Not Affected	link			cisagov	2021-12-15
Dell	Dell Display Manager 2.0 for Windows / macOS			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC AppSync			Not Affected	link			cisagov	2021-12-15

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Dell	Dell EMC Avamar	N/A		Affected	link	Patch expected by 12/20/21 See DSA-2021-305		cisagov	2021-12-15
Dell	Dell EMC BSN Controller Node			Unknown	link			cisagov	2021-12-15
Dell	Dell EMC Cloud Disaster Recovery			Affected	link	Patch pending		cisagov	2021-12-15
Dell	Dell EMC Cloudboost			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC CloudLink			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC Container Storage Modules			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC Data Computing Appliance (DCA)			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC Data Protection Advisor			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC Data Protection Central			Unknown	link	See DSA-2021-269		cisagov	2021-12-15
Dell	Dell EMC Data Protection Search			Affected	link	See DSA-2021-279		cisagov	2021-12-15
Dell	Dell EMC DataIQ	Versions before 19.5.0.7		Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC Disk Library for Mainframe			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC ECS			Unknown	link	Patch expected by 12/18/21 See DSA-2021-278		cisagov	2021-12-15
Dell	Dell EMC Enterprise Storage Analytics for vRealize Operations			Affected	link			cisagov	2021-12-15
Dell	Dell EMC GeoDrive			Not Affected	link			cisagov	2021-12-15

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Dell	Dell EMC Integrated System for Azure Stack HCI	N/A		Affected	link	"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: Patch pending		cisagov	2021-12-15
Dell	Dell EMC Integrated System for Microsoft Azure Stack Hub	N/A		Affected	link			cisagov	2021-12-15
Dell	Dell EMC Isilon InsightIQ			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC License Manager			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC Metro Node	7.0.x		Affected	link	See DSA-2021-308		cisagov	2021-12-15
Dell	Dell EMC NetWorker Server	"19.5.x 19.4.x 19.3.x"		Affected	link	Patch expected by 12/20/21		cisagov	2021-12-15
Dell	Dell EMC NetWorker Virtual Edition	"19.5.x 19.4.x 19.3.x"		Affected	link	Patch expected by 12/20/21		cisagov	2021-12-15
Dell	Dell EMC Networking Onie			Not Affected	link			cisagov	2021-12-15



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Dell	Dell EMC Networking Virtual Edge Platform	“with Versa Concerto with Versa Analytics with Versa Concerto Director”		Affected	link	See DSA-2021-304		cisagov	2021-12-15
Dell	with VersaOS Dell EMC OpenManage Ansible Modules			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC OpenManage integration for Splunk			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC OpenManage Integration for VMware vCenter			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC OpenManage Management pack for vRealize Operations			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC OpenManage Operations Connector for Micro Focus Operations Bridge Manager			Not Affected	link			cisagov	2021-12-15
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	link	Patch pending		cisagov	2021-12-15
Dell	Dell EMC PowerFlex Rack	N/A		Affected	link	Patch pending		cisagov	2021-12-15
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	link	Patch pending		cisagov	2021-12-15
Dell	Dell EMC PowerPath			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC PowerPath Management Appliance			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC PowerProtect Cyber Recovery			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC PowerProtect Data Manager	All versions 19.9 and earlier		Affected	link	Patch pending		cisagov	2021-12-15
Dell	Dell EMC PowerProtect DP Series Appliance (iDPA)	2.7.0 and earlier		Affected	link	Patch pending		cisagov	2021-12-15
Dell	Dell EMC PowerScale OneFS			Not Affected	link			cisagov	2021-12-15

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Dell	Dell EMC PowerShell for PowerMax			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC PowerShell for Powerstore			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC PowerShell for Unity			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC PowerStore			Unknown	link	Patch expected by 12/23/21		cisagov	2021-12-15
Dell	Dell EMC PowerVault MD3 Series Storage Arrays			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC PowerVault ME4 Series Storage Arrays			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC RecoverPoint Classic	All 5.1.x and later versions		Affected	link	Patch pending		cisagov	2021-12-15
Dell	Dell EMC RecoverPoint for Virtual Machine	All 5.0.x and later versions		Affected	link	Patch pending		cisagov	2021-12-15
Dell	Dell EMC Repository Manager (DRM)			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC Ruckus SmartZone 100 Controller			Unknown	link	See DSA-2021-303		cisagov	2021-12-15
Dell	Dell EMC Ruckus SmartZone 300 Controller			Unknown	link	See DSA-2021-303		cisagov	2021-12-15
Dell	Dell EMC Ruckus Virtual Software			Unknown	link	See DSA-2021-303		cisagov	2021-12-15
Dell	Dell EMC SourceOne			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC SRM vApp	Versions before 4.6.0.2		Affected	link	Patch expected by 1/25/2022		cisagov	2021-12-15
Dell	Dell EMC Streaming Data Platform			Unknown	link	Patch expected by 12/18/21		cisagov	2021-12-15
Dell	Dell EMC Systems Update (DSU)			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC Unisphere 360			Not Affected	link			cisagov	2021-12-15

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Dell	Dell EMC Unity			Unknown	link	Patch expected by 12/29/21		cisagov	2021-12-15
Dell	Dell EMC Virtual Storage Integrator			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC VPLEX			Not Affected	link			cisagov	2021-12-15
Dell	Dell EMC VxRail	"4.5.x 4.7.x 7.0.x"		Affected	link	Patch pending		cisagov	2021-12-15
Dell	Dell EMC XtremIO			Not Affected	link			cisagov	2021-12-15
Dell	Dell Encryption Enterprise*			Not Affected	link			cisagov	2021-12-15
Dell	Dell Encryption Personal*			Not Affected	link			cisagov	2021-12-15
Dell	Dell Endpoint Security Suite Enterprise*			Not Affected	link			cisagov	2021-12-15
Dell	Dell Hybrid Client			Not Affected	link			cisagov	2021-12-15
Dell	Dell ImageAssist			Not Affected	link			cisagov	2021-12-15
Dell	Dell Insights Client			Not Affected	link			cisagov	2021-12-15
Dell	Dell Linux Assistant			Not Affected	link			cisagov	2021-12-15
Dell	Dell Mobile Connect			Not Affected	link			cisagov	2021-12-15
Dell	Dell Monitor ISP (Windows/Mac/Linux)			Not Affected	link			cisagov	2021-12-15
Dell	Dell Monitor SDK			Not Affected	link			cisagov	2021-12-15
Dell	Dell Networking X-Series			Not Affected	link			cisagov	2021-12-15
Dell	Dell Open Manage Mobile			Not Affected	link			cisagov	2021-12-15
Dell	Dell Open Manage Server Administrator			Not Affected	link			cisagov	2021-12-15
Dell	Dell Open Management Enterprise - Modular	<1.40.10		Affected	link	See DSA-2021-268		cisagov	2021-12-15
Dell	Dell OpenManage Change Management			Not Affected	link			cisagov	2021-12-15
Dell	Dell OpenManage Enterprise Power Manager Plugin			Not Affected	link			cisagov	2021-12-15
Dell	Dell Optimizer			Not Affected	link			cisagov	2021-12-15

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Dell	Dell OS Recovery Tool			Not Affected	link			cisagov	2021-12-15
Dell	Dell Peripheral Manager 1.4 / 1.5 for Windows			Not Affected	link			cisagov	2021-12-15
Dell	Dell Platform Service			Not Affected	link			cisagov	2021-12-15
Dell	Dell Power Manager			Not Affected	link			cisagov	2021-12-15
Dell	Dell Power Manager Lite			Not Affected	link			cisagov	2021-12-15
Dell	Dell Precision Optimizer			Not Affected	link			cisagov	2021-12-15
Dell	Dell Precision Optimizer for Linux			Not Affected	link			cisagov	2021-12-15
Dell	Dell Premier Color			Not Affected	link			cisagov	2021-12-15
Dell	Dell Recovery (Linux)			Not Affected	link			cisagov	2021-12-15
Dell	Dell Remediation Platform			Not Affected	link			cisagov	2021-12-15
Dell	Dell Remote Execution Engine (DRONE)			Not Affected	link			cisagov	2021-12-15
Dell	Dell Security Advisory Update - DSA-2021-088			Not Affected	link			cisagov	2021-12-15
Dell	Dell Security Management Server & Dell Security Management Server Virtual*			Not Affected	link			cisagov	2021-12-15
Dell	Dell Support-Assist SOS			Not Affected	link			cisagov	2021-12-15
Dell	Dell Thin OS			Not Affected	link			cisagov	2021-12-15
Dell	Dell Threat Defense			Not Affected	link			cisagov	2021-12-15
Dell	Dell True Color			Not Affected	link			cisagov	2021-12-15
Dell	Dell Trusted Device			Not Affected	link			cisagov	2021-12-15
Dell	Dell Update			Not Affected	link			cisagov	2021-12-15
Dell	DellEMC OpenManage Enterprise Services			Unknown	link	Patch expected by 12/20/21		cisagov	2021-12-15
Dell	Dream Catcher			Not Affected	link			cisagov	2021-12-15
Dell	DUP Creation Service			Not Affected	link			cisagov	2021-12-15
Dell	DUP Framework (ISG)			Not Affected	link			cisagov	2021-12-15

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Dell	Embedded NAS			Not Affected	link			cisagov	2021-12-15
Dell	Embedded Service Enabler			Not Affected	link			cisagov	2021-12-15
Dell	Enterprise Hybrid Cloud			Unknown	link	link		cisagov	2021-12-15
Dell	Equallogic PS			Not Affected	link			cisagov	2021-12-15
Dell	Fluid FS			Not Affected	link			cisagov	2021-12-15
Dell	iDRAC Service Module (iSM)			Not Affected	link			cisagov	2021-12-15
Dell	Infinity MLK (firmware)			Not Affected	link			cisagov	2021-12-15
Dell	Integrated Dell Remote Access Controller (iDRAC)			Not Affected	link			cisagov	2021-12-15
Dell	ISG Accelerators			Not Affected	link			cisagov	2021-12-15
Dell	ISG Board & Electrical			Not Affected	link			cisagov	2021-12-15
Dell	IsilonSD Management Server			Not Affected	link			cisagov	2021-12-15
Dell	IVE-WinDiag			Not Affected	link			cisagov	2021-12-15
Dell	Mainframe Enablers			Not Affected	link			cisagov	2021-12-15
Dell	My Dell			Not Affected	link			cisagov	2021-12-15
Dell	MyDell Mobile			Not Affected	link			cisagov	2021-12-15
Dell	NetWorker Management Console			Not Affected	link			cisagov	2021-12-15
Dell	Networking BIOS			Not Affected	link			cisagov	2021-12-15
Dell	Networking DIAG			Not Affected	link			cisagov	2021-12-15
Dell	Networking N-Series			Not Affected	link			cisagov	2021-12-15
Dell	Networking OS 10			Not Affected	link			cisagov	2021-12-15
Dell	Networking OS9			Not Affected	link			cisagov	2021-12-15
Dell	Networking SD-WAN Edge			Not Affected	link			cisagov	2021-12-15
Dell	Networking SD-WAN W-Series			Not Affected	link			cisagov	2021-12-15
Dell	Networking X-Series			Not Affected	link			cisagov	2021-12-15
Dell	OMIMSSC (OpenMan-age Integration for Microsoft System Center)			Not Affected	link			cisagov	2021-12-15
Dell	OMNIA			Not Affected	link			cisagov	2021-12-15

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Dell	OpenManage Connections - Nagios			Not Affected	link			cisagov	2021-12-15
Dell	OpenManage Connections - ServiceNow			Not Affected	link			cisagov	2021-12-15
Dell	OpenManage Enterprise			Unknown	link	Patch expected by 12/19/21		cisagov	2021-12-15
Dell	OpenManage Integration for Microsoft System Center for System Center Operations Manager			Not Affected	link			cisagov	2021-12-15
Dell	OpenManage Integration with Microsoft Windows Admin Center			Not Affected	link			cisagov	2021-12-15
Dell	OpenManage Network Integration			Not Affected	link			cisagov	2021-12-15
Dell	PowerConnect N3200			Not Affected	link			cisagov	2021-12-15
Dell	PowerConnect PC2800			Not Affected	link			cisagov	2021-12-15
Dell	PowerConnect PC8100			Not Affected	link			cisagov	2021-12-15
Dell	PowerEdge BIOS			Not Affected	link			cisagov	2021-12-15
Dell	PowerEdge Operating Systems			Not Affected	link			cisagov	2021-12-15
Dell	PowerTools Agent			Not Affected	link			cisagov	2021-12-15
Dell	PPDM Kubernetes			Not Affected	link			cisagov	2021-12-15
Dell	cProxy PPDM			Not Affected	link			cisagov	2021-12-15
Dell	VMware vProxy			Not Affected	link			cisagov	2021-12-15
Dell	Redtail			Not Affected	link			cisagov	2021-12-15
Dell	Remotely Anywhere			Not Affected	link			cisagov	2021-12-15
Dell	Riptide (firmware)			Not Affected	link			cisagov	2021-12-15
Dell	Rugged Control Center (RCC)			Not Affected	link			cisagov	2021-12-15
Dell	SD ROM Utility			Not Affected	link			cisagov	2021-12-15
Dell	SDNAS			Not Affected	link			cisagov	2021-12-15
Dell	Secure Connect Gateway (SCG) Appliance	"5.00.00 5.00.05 and 4.0.06 and earlier versions (OVF and VHD)"		Affected	link	See DSA-2021-282		cisagov	2021-12-15

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Dell	Secure Connect Gateway (SCG) Policy Manager	“5.00.00.10 5.00.05.10”		Affected	link	See DSA-2021-281		cisagov	2021-12-15
Dell	Server Storage			Not Affected	link			cisagov	2021-12-15
Dell	Smart Fabric Storage Software			Not Affected	link			cisagov	2021-12-15
Dell	SmartByte			Not Affected	link			cisagov	2021-12-15
Dell	SMI-S			Not Affected	link			cisagov	2021-12-15
Dell	Software RAID			Not Affected	link			cisagov	2021-12-15
Dell	Solutions Enabler			Not Affected	link			cisagov	2021-12-15
Dell	Solutions Enabler vApp			Not Affected	link			cisagov	2021-12-15
Dell	Sonic			Not Affected	link			cisagov	2021-12-15
Dell	SRS Policy Manager	7		Affected	link	Patch pending		cisagov	2021-12-15
Dell	SRS VE			Not Affected	link			cisagov	2021-12-15
Dell	Storage Center - Dell Storage Manager			Unknown	link	Patch pending		cisagov	2021-12-15
Dell	Storage Center OS and additional SC applications unless otherwise noted			Not Affected	link			cisagov	2021-12-15
Dell	SupportAssist Client			Not Affected	link			cisagov	2021-12-15
Dell	Commercial SupportAssist Client			Not Affected	link			cisagov	2021-12-15
Dell	Consumer SupportAssist Enterprise			Unknown	link	Patch expected by 12/23/21		cisagov	2021-12-15
Dell	UCC Edge			Not Affected	link			cisagov	2021-12-15
Dell	Unisphere Central			Unknown	link	Patch expected by 1/10/2022		cisagov	2021-12-15
Dell	Unisphere for PowerMax			Not Affected	link			cisagov	2021-12-15
Dell	Unisphere for PowerMax vApp			Not Affected	link			cisagov	2021-12-15
Dell	Unisphere for VMAX			Not Affected	link			cisagov	2021-12-15
Dell	Unisphere for VNX			Not Affected	link			cisagov	2021-12-15
Dell	Update Manager Plugin			Not Affected	link			cisagov	2021-12-15

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Dell	Vblock			Unknown	link	Patch pending See vce6771 (requires customer login)		cisagov	2021-12-15
Dell	ViPR Controller			Not Affected	link			cisagov	2021-12-15
Dell	VMware vRealize Automation 8.x	“8.2 8.3 8.4 8.5 and 8.6”		Affected	link	Patch expected by 12/19/21		cisagov	2021-12-15
Dell	VMware vRealize Orchestrator 8.x	“8.2 8.3 8.4 8.5 and 8.6”		Affected	link	Patch expected by 12/19/21		cisagov	2021-12-15
Dell	VNX1			Not Affected	link			cisagov	2021-12-15
Dell	VNX2			Not Affected	link			cisagov	2021-12-15
Dell	VNXe 1600	Versions 3.1.16.10220572 and earlier		Affected	link	Patch expected by 12/19/21		cisagov	2021-12-15
Dell	VNXe 3200	Version 3.1.15.10216415 and earlier		Affected	link	Patch expected by 12/19/21		cisagov	2021-12-15
Dell	VPLEX VS2/VS6 / VPLEX			Not Affected	link			cisagov	2021-12-15
Dell	Witness vRealize Data Protection Extension Data Management			Unknown	link	Patch expected by 12/19/21		cisagov	2021-12-15
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	link	Patch expected by 12/19/21		cisagov	2021-12-15
Dell	vRealize Orchestrator (vRO) Plug-ins for Dell EMC Storage	Various		Affected	link	See DSA-2021-300		cisagov	2021-12-15
Dell	vRO Plugin for Dell EMC PowerMax	Version 1.2.3 or earlier		Affected	link	See DSA-2021-300		cisagov	2021-12-15
Dell	vRO Plugin for Dell EMC PowerScale	Version 1.1.0 or earlier		Affected	link	See DSA-2021-300		cisagov	2021-12-15
Dell	vRO Plugin for Dell EMC PowerStore	Version 1.1.4 or earlier		Affected	link	See DSA-2021-300		cisagov	2021-12-15
Dell	vRO Plugin for Dell EMC Unity	Version 1.0.6 or earlier		Affected	link	See DSA-2021-300		cisagov	2021-12-15
Dell	vRO Plugin for Dell EMC XtremIO	Version 4.1.2 or earlier		Affected	link	See DSA-2021-300		cisagov	2021-12-15



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Dell	Vsan Ready Nodes			Not Affected	link			cisagov	2021-12-15
Dell	VxBlock			Unknown	link	“Patch pending See vce6771 (requires customer login)”		cisagov	2021-12-15
Dell	Warnado MLK (firmware)			Not Affected	link			cisagov	2021-12-15
Dell	Wyse Management Suite	<3.5		Affected	link	See DSA-2021-267		cisagov	2021-12-15
Dell	Wyse Proprietary OS (ThinOS)			Not Affected	link			cisagov	2021-12-15
Dell	Wyse Windows Embedded Suite			Not Affected	link			cisagov	2021-12-15
Deltares	Delft-FEWS		>2018.02	Fixed	link	Mitigations Only		cisagov	2021-12-22
Denequa Device42				Unknown	link			cisagov	2022-01-12
Devolutions	All products			Unknown	link			cisagov	2022-01-12
Diebold Nixdorf				Unknown	link			cisagov	2022-01-12
Digi International	AnywhereUSB Manager			Unknown	link			cisagov	2021-12-21
Digi International	ARMT			Unknown	link			cisagov	2021-12-21
Digi International	Aview			Unknown	link			cisagov	2021-12-21
Digi International	AVWOB			Unknown	link			cisagov	2021-12-21
Digi International	CTEK G6200 family			Unknown	link			cisagov	2021-12-21
Digi International	CTEK SkyCloud			Unknown	link			cisagov	2021-12-21
Digi International	CTEK Z45 family			Unknown	link			cisagov	2021-12-21
Digi International	Digi 54xx family			Unknown	link			cisagov	2021-12-21
Digi International	Digi 63xx family			Unknown	link			cisagov	2021-12-21
Digi International	Digi Any-whereUSB (G2) family			Unknown	link			cisagov	2021-12-21
Digi International	Digi Any-whereUSB Plus family			Unknown	link			cisagov	2021-12-21
Digi International	Digi Connect EZ family			Unknown	link			cisagov	2021-12-21
Digi International	Digi Connect family			Unknown	link			cisagov	2021-12-21
Digi International	Digi Connect IT family			Unknown	link			cisagov	2021-12-21
Digi International	Digi Connect Sensor family			Unknown	link			cisagov	2021-12-21
Digi International	Digi Connect WS family			Unknown	link			cisagov	2021-12-21
Digi International	Digi ConnectPort family			Unknown	link			cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Digi International	Digi ConnectPort LTS family			Unknown	link			cisagov	2021-12-21
Digi International	Digi Embedded Android			Unknown	link			cisagov	2021-12-21
Digi International	Digi Embedded Yocto			Unknown	link			cisagov	2021-12-21
Digi International	Digi EX routers			Unknown	link			cisagov	2021-12-21
Digi International	Digi IX routers			Unknown	link			cisagov	2021-12-21
Digi International	Digi LR54			Unknown	link			cisagov	2021-12-21
Digi International	Digi Navigator			Unknown	link			cisagov	2021-12-21
Digi International	Digi One family			Unknown	link			cisagov	2021-12-21
Digi International	Digi Passport family			Unknown	link			cisagov	2021-12-21
Digi International	Digi PortServer TS family			Unknown	link			cisagov	2021-12-21
Digi International	Digi Remote Manager			Unknown	link			cisagov	2021-12-21
Digi International	Digi TX routers			Unknown	link			cisagov	2021-12-21
Digi International	Digi WR11			Unknown	link			cisagov	2021-12-21
Digi International	Digi WR21			Unknown	link			cisagov	2021-12-21
Digi International	Digi WR31			Unknown	link			cisagov	2021-12-21
Digi International	Digi WR44R/RR			Unknown	link			cisagov	2021-12-21
Digi International	Digi WR54			Unknown	link			cisagov	2021-12-21
Digi International	Digi WR64			Unknown	link			cisagov	2021-12-21
Digi International	Digi Xbee			Unknown	link			cisagov	2021-12-21
Digi International	mobile app			Unknown	link			cisagov	2021-12-21
Digi International	Lighthouse			Unknown	link			cisagov	2021-12-21
Digi International	Realport			Unknown	link			cisagov	2021-12-21
Digi International	Remote Hub Config Utility			Unknown	link			cisagov	2021-12-21
Digicert				Unknown	link			cisagov	2022-01-12
Digital Alert Systems	Digital AI			Unknown	link			cisagov	2022-01-12
	All			Unknown	link	Formerly Monroe Electronics, Inc.		cisagov	2022-01-05
DNSFilter				Unknown	link			cisagov	2022-01-12
Docker				Unknown	link			cisagov	2022-01-12
Docusign				Unknown	link			cisagov	2022-01-12
DrayTek	Vigor Routers, Access Points, Switches, VigorACS Central Management Software, MyVigor Platform			Unknown	link			cisagov	2021-12-15

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
DSpace				Unknown	link			cisagov	2022-01-12
Dynatrace	ActiveGate			Unknown	link			cisagov	2021-12-21
Dynatrace	Dynatrace Extensions			Unknown	link	Please see Dynatrace Communication for details		cisagov	2021-12-21
Dynatrace	FedRamp SAAS			Unknown	link			cisagov	2021-12-21
Dynatrace	Managed cluster nodes			Unknown	link	Please see Dynatrace Communication for details		cisagov	2021-12-21
Dynatrace	OneAgent			Unknown	link			cisagov	2021-12-21
Dynatrace	SAAS			Unknown	link			cisagov	2021-12-21
Dynatrace	Synthetic Private ActiveGate			Unknown	link	Please see Dynatrace Communication for details		cisagov	2021-12-21
Dynatrace	Synthetic public locations			Unknown	link			cisagov	2021-12-21
EasyRedmine				Unknown	link			cisagov	2022-01-12
Eaton	Undisclosed	Undisclosed		Affected	link	Doesn't openly disclose what products are affected or not for quote 'security purposes'. Needs email registration. No workaround provided due to registration wall.		cisagov	2022-01-12
EclecticIQ				Unknown	link			cisagov	2022-01-12
Eclipse Foundation				Unknown	link			cisagov	2022-01-12
Edwards				Unknown	link			cisagov	2022-01-06
EFI				Unknown	link			cisagov	2022-01-12
EGroupware				Unknown	link			cisagov	2022-01-12
Elastic	APM Java Agent			Unknown	link			cisagov	2021-12-15
Elastic	APM Server			Unknown	link			cisagov	2021-12-15
Elastic	Beats			Unknown	link			cisagov	2021-12-15
Elastic	Cmd			Unknown	link			cisagov	2021-12-15
Elastic	Elastic Agent			Unknown	link			cisagov	2021-12-15
Elastic	Elastic Cloud			Unknown	link			cisagov	2021-12-15
Elastic	Elastic Cloud Enterprise			Unknown	link			cisagov	2021-12-15
Elastic	Elastic Cloud Enterprise			Unknown	link			cisagov	2021-12-15
Elastic	Elastic Cloud on Kubernetes			Unknown	link			cisagov	2021-12-15
Elastic	Elastic Endgame			Unknown	link			cisagov	2021-12-15

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Elastic	Elastic Maps Service	5, 6, 8		Unknown	link			cisagov	2021-12-15
Elastic	Elasticsearch			Affected	link			cisagov	2021-12-15
Elastic	Endpoint Security			Unknown	link			cisagov	2021-12-15
Elastic	Enterprise Search	<6.8.21, <7.16.1		Unknown	link			cisagov	2021-12-15
Elastic	Fleet Server			Unknown	link			cisagov	2021-12-15
Elastic	Kibana			Unknown	link			cisagov	2021-12-15
Elastic	Logstash			Affected	link			cisagov	2021-12-15
Elastic	Machine Learning			Unknown	link			cisagov	2021-12-15
ElasticSearch	all products			Unknown				cisagov	2022-01-12
Elastic	Swifttype			Unknown	link			cisagov	2021-12-15
Ellucian	Admin			Unknown	link			cisagov	2021-12-17
Ellucian	Banner Analytics			Unknown	link			cisagov	2021-12-17
Ellucian	Banner Document Management (includes Banner Document Retention)			Unknown	link			cisagov	2021-12-17
Ellucian	Banner Event Publisher			Unknown	link			cisagov	2021-12-17
Ellucian	Banner Integration for eLearning			Unknown	link			cisagov	2021-12-17
Ellucian	Banner Integration for eProcurement			Unknown	link			cisagov	2021-12-17
Ellucian	Banner Self Service			Unknown	link			cisagov	2021-12-17
Ellucian	Banner Workflow			Unknown	link			cisagov	2021-12-17
Ellucian	Colleague			Unknown	link			cisagov	2021-12-17
Ellucian	Colleague Analytics			Unknown	link			cisagov	2021-12-17
Ellucian	CRM			Unknown	link			cisagov	2021-12-17
Ellucian	Advance CRM Advise			Unknown	link			cisagov	2021-12-17
Ellucian	CRM Recruit			Unknown	link			cisagov	2021-12-17
Ellucian	Ellucian Advance Web Connector			Unknown	link			cisagov	2021-12-17
Ellucian	Ellucian Data Access			Unknown	link			cisagov	2021-12-17
Ellucian	Ellucian Design Path			Unknown	link			cisagov	2021-12-17
Ellucian	Ellucian Portal			Unknown	link			cisagov	2021-12-17
Ellucian	Ellucian ePrint			Unknown	link			cisagov	2021-12-17
Ellucian	Ellucian Ethos API & API Management Center			Unknown	link			cisagov	2021-12-17

On-prem and cloud deployments expect fixed 12/18/2021

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Ellucian	Ellucian Ethos Extend			Unknown	link			cisagov	2021-12-17
Ellucian	Ellucian Ethos			Unknown	link			cisagov	2021-12-17
Ellucian	Integration Ellucian eTranscripts			Unknown	link			cisagov	2021-12-17
Ellucian	Ellucian Experience			Unknown	link			cisagov	2021-12-17
Ellucian	Ellucian Intelligent Platform (ILP)			Unknown	link			cisagov	2021-12-17
Ellucian	Ellucian International Student and Scholar Management (ISSM)			Unknown	link			cisagov	2021-12-17
Ellucian	Ellucian Message Service (EMS)			Unknown	link			cisagov	2021-12-17
Ellucian	Ellucian Messaging Adapter (EMA)			Unknown	link			cisagov	2021-12-17
Ellucian	Ellucian Mobile			Unknown	link			cisagov	2021-12-17
Ellucian	Ellucian Payment Gateway			Unknown	link			cisagov	2021-12-17
Ellucian	Ellucian PowerCampus			Unknown	link			cisagov	2021-12-17
Ellucian	Ellucian Solution Manager			Unknown	link			cisagov	2021-12-17
Ellucian	Ellucian Workflow			Unknown	link			cisagov	2021-12-17
Ellucian	Enterprise Identity Services(BEIS)			Unknown	link			cisagov	2021-12-17
Emerson	148 Temperature Transmitter			Unknown	link			cisagov	2021-12-17
Emerson	2051 Pressure Transmitter			Unknown	link			cisagov	2021-12-17
Emerson	Family 2088 Pressure Transmitter			Unknown	link			cisagov	2021-12-17
Emerson	Family 2090F/2090P Pressure Transmitters			Unknown	link			cisagov	2021-12-17
Emerson	215 Pressure Sensor			Unknown	link			cisagov	2021-12-17
Emerson	Module 248 Configuration			Unknown	link			cisagov	2021-12-17
Emerson	Application 248 Temperature Transmitter			Unknown	link			cisagov	2021-12-17
Emerson	3051 & 3051S Pressure transmitter families			Unknown	link			cisagov	2021-12-17

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Emerson	3144P Temperature Transmitter			Unknown	link			cisagov	2021-12-17
Emerson	326P Pressure Transmitter			Unknown	link			cisagov	2021-12-17
Emerson	326T Temperature Transmitter			Unknown	link			cisagov	2021-12-17
Emerson	327T Temperature Transmitter			Unknown	link			cisagov	2021-12-17
Emerson	4088 Pressure Transmitter			Unknown	link			cisagov	2021-12-17
Emerson	4088 Upgrade Utility			Unknown	link			cisagov	2021-12-17
Emerson	4600 Pressure Transmitter			Unknown	link			cisagov	2021-12-17
Emerson	4732 Endeavor			Unknown	link			cisagov	2021-12-17
Emerson	4732 Endeavor			Unknown	link			cisagov	2021-12-17
Emerson	550 PT Pressure Transmitter			Unknown	link			cisagov	2021-12-17
Emerson	5726 Transmitter			Unknown	link			cisagov	2021-12-17
Emerson	5726 Transmitter			Unknown	link			cisagov	2021-12-17
Emerson	644 Temperature Transmitter			Unknown	link			cisagov	2021-12-17
Emerson	648 Temperature Transmitter			Unknown	link			cisagov	2021-12-17
Emerson	848T Temperature Transmitter			Unknown	link			cisagov	2021-12-17
Emerson	Combustion: OCX OXT 6888 CX1100 6888Xi			Unknown	link			cisagov	2021-12-17
Emerson	CT2211 QCL Aerosol Microleak Detection System			Unknown	link			cisagov	2021-12-17
Emerson	CT3000 QCL Automotive OEM Gas Analyzer			Unknown	link			cisagov	2021-12-17
Emerson	CT4000 QCL Marine OEM Gas Analyzer			Unknown	link			cisagov	2021-12-17
Emerson	CT4215 QCL Packaging Leak Detection System			Unknown	link			cisagov	2021-12-17
Emerson	CT4400 QCL General Purpose Continuous Gas Analyzer			Unknown	link			cisagov	2021-12-17
Emerson	CT4404 QCL pMDI Leak Detection Analyzer			Unknown	link			cisagov	2021-12-17

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Emerson	CT5100 QCL Field Housing Continuous Gas Analyzer			Unknown	link			cisagov	2021-12-17
Emerson	CT5400 QCL General Purpose Continuous Gas Analyzer			Unknown	link			cisagov	2021-12-17
Emerson	CT5800 QCL Flameproof Housing Continuous Gas Analyzer			Unknown	link			cisagov	2021-12-17
Emerson	DHNC1 DHNC2			Unknown	link			cisagov	2021-12-17
Emerson	DHNC1 DHNC2			Unknown	link			cisagov	2021-12-17
Emerson	Emerson Aperio software			Unknown	link			cisagov	2021-12-17
Emerson	Engineering Assistant 5.x & 6.x			Unknown	link			cisagov	2021-12-17
Emerson	Fieldwatch and Service consoles			Unknown	link			cisagov	2021-12-17
Emerson	Fieldwatch and Service consoles			Unknown	link			cisagov	2021-12-17
Emerson	Flame Detection: 975UF & 975UR Infrared Flame Detectors 975HR Infrared Hydrogen Flame Detector 975MR Multi- Spectrum Infrared Flame Detector			Unknown	link			cisagov	2021-12-17
Emerson	Flarecheck FlowCheck Flowel & PWAM software			Unknown	link			cisagov	2021-12-17
Emerson	Flarecheck FlowCheck Flowel & PWAM software			Unknown	link			cisagov	2021-12-17
Emerson	Gas Analysis: X-STREAM Enhanced (XEGP XEGK XEGC XEGF XEFD XECLD)			Unknown	link			cisagov	2021-12-17

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Emerson	Gas Analysis: X-STREAM Enhanced (XEGP XEGK XEGC XEGF XEFD XECLD)			Unknown	link			cisagov	2021-12-17
Emerson	Gas Chro- matographs: M500/2350A MON2000 700XA/1500XA 370XA MON2020			Unknown	link			cisagov	2021-12-17
Emerson	Gas Chro- matographs: M500/2350A MON2000 700XA/1500XA 370XA MON2020			Unknown	link			cisagov	2021-12-17
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			Unknown	link			cisagov	2021-12-17
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			Unknown	link			cisagov	2021-12-17
Emerson	Incus Ultrasonic gas leak detector			Unknown	link			cisagov	2021-12-17
Emerson	K-Series Coriolis Transmitters			Unknown	link			cisagov	2021-12-17
Emerson	K-Series Coriolis Transmitters			Unknown	link			cisagov	2021-12-17
Emerson	Liquid Transmitters: 5081 1066 1056 1057 56			Unknown	link			cisagov	2021-12-17



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Emerson	Mark III Gas and Liquid USM			Unknown	link			cisagov	2021-12-17
Emerson	Mark III Gas and Liquid USM			Unknown	link			cisagov	2021-12-17
Emerson	MPFM2600 & MPFM5726			Unknown	link			cisagov	2021-12-17
Emerson	MPFM2600 & MPFM5726			Unknown	link			cisagov	2021-12-17
Emerson	Plantweb Advisor for Metrology and Metering Suite SDK			Unknown	link			cisagov	2021-12-17
Emerson	Plantweb Advisor for Metrology and Metering Suite SDK			Unknown	link			cisagov	2021-12-17
Emerson	Prolink Configuration Software			Unknown	link			cisagov	2021-12-17
Emerson	Prolink Configuration Software			Unknown	link			cisagov	2021-12-17
Emerson	Prolink Mobile Application & ProcessViz Software			Unknown	link			cisagov	2021-12-17
Emerson	Prolink Mobile Application & ProcessViz Software			Unknown	link			cisagov	2021-12-17
Emerson	Rosemount 2230 Graphical Field Display			Unknown	link			cisagov	2021-12-17
Emerson	Rosemount 2240S Multi-input Temperature Transmitter			Unknown	link			cisagov	2021-12-17
Emerson	Rosemount 2410 Tank Hub			Unknown	link			cisagov	2021-12-17
Emerson	Rosemount 2460 System Hub			Unknown	link			cisagov	2021-12-17
Emerson	Rosemount 3490 Controller			Unknown	link			cisagov	2021-12-17
Emerson	Rosemount CMS/IOU 61			Unknown	link			cisagov	2021-12-17
Emerson	Rosemount CMS/SCU 51/SCC			Unknown	link			cisagov	2021-12-17
Emerson	Rosemount CMS/WSU 51/SWF 51			Unknown	link			cisagov	2021-12-17
Emerson	Rosemount IO-Link Assistant			Unknown	link			cisagov	2021-12-17

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Emerson	Rosemount Level Detectors (21xx)			Unknown	link			cisagov	2021-12-17
Emerson	Rosemount Level Transmitters (14xx 33xx 53xx 54xx 56xx)			Unknown	link			cisagov	2021-12-17
Emerson	Rosemount Radar Configuration Tool			Unknown	link			cisagov	2021-12-17
Emerson	Rosemount Radar Level Gauges (Pro 39xx 59xx)			Unknown	link			cisagov	2021-12-17
Emerson	Rosemount RadarMaster and RadarMaster Plus			Unknown	link			cisagov	2021-12-17
Emerson	Rosemount Tank Radar Gauges (TGUxx)			Unknown	link			cisagov	2021-12-17
Emerson	Rosemount TankMaster and TankMaster Mobile			Unknown	link			cisagov	2021-12-17
Emerson	Spectrex family Flame Detectors and Rosemount 975 flame detector			Unknown	link			cisagov	2021-12-17
Emerson	USM 3410 and 3810 Series Ultrasonic Transmitters			Unknown	link			cisagov	2021-12-17
Emerson	USM 3410 and 3810 Series Ultrasonic Transmitters			Unknown	link			cisagov	2021-12-17
Emerson	Vortex and Magmeter Transmitters			Unknown	link			cisagov	2021-12-17
Emerson	Vortex and Magmeter Transmitters			Unknown	link			cisagov	2021-12-17
Emerson	WCM SWGM			Unknown	link			cisagov	2021-12-17
Emerson	WCM SWGM			Unknown	link			cisagov	2021-12-17
EnterpriseDT				Unknown	link			cisagov	2022-01-12
ESET				Unknown	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
ESRI	ArcGIS Data Store		All	Fixed	<a href="#">link</a>	Requires script re-mediation. ESRI has created scripts to remove the JndiLookup class, but has not issued patches to upgrade the Log4j versions		cisagov	2021-12-17
ESRI	ArcGIS Enterprise		All	Fixed	<a href="#">link</a>	Requires script re-mediation. ESRI has created scripts to remove the JndiLookup class, but has not issued patches to upgrade the Log4j versions		cisagov	2021-12-17
ESRI	ArcGIS GeoEvent Server		All	Fixed	<a href="#">link</a>	Requires script re-mediation. ESRI has created scripts to remove the JndiLookup class, but has not issued patches to upgrade the Log4j versions		cisagov	2021-12-17
ESRI	ArcGIS Server		All	Fixed	<a href="#">link</a>	Requires script re-mediation. ESRI has created scripts to remove the JndiLookup class, but has not issued patches to upgrade the Log4j versions		cisagov	2021-12-17

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
ESRI	ArcGIS Workflow Manager Server		All	Fixed	link	Requires script re-mediation. ESRI has created scripts to remove the JndiLookup class, but has not issued patches to upgrade the Log4j versions		cisagov	2021-12-17
ESRI	Portal for ArcGIS		All	Fixed	link	Requires script re-mediation. ESRI has created scripts to remove the JndiLookup class, but has not issued patches to upgrade the Log4j versions		cisagov	2021-12-17
Estos				Unknown	link			cisagov	2022-01-12
Evolveum				Unknown	link			cisagov	2022-01-12
Midpoint									
Ewon				Unknown	link			cisagov	2022-01-12
Exabeam				Unknown	link	This advisory is available to customers only and has not been reviewed by CISA		cisagov	2022-01-12
Exact				Unknown	link			cisagov	2022-01-12
Exivity				Unknown	link			cisagov	2022-01-12
ExtraHop	Reveal(x)	<=8.4.6, <=8.5.3, <=8.6.4		Affected	link	Versions >8.4.7, >8.5.4, >8.6.5 and >=8.7 are fixed.		cisagov	2021-12-21
eXtreme				Unknown	link			cisagov	2022-01-12
Hosting									
Extreme				Unknown	link			cisagov	2022-01-12
Networks									
Extron				Unknown	link			cisagov	2022-01-12
F-Secure	Elements Connector			Unknown	link			cisagov	2022-01-12
F-Secure	Endpoint	13-15		Affected	link			cisagov	2022-01-12
F-Secure	Proxy Messaging Security Gateway			Unknown	link			cisagov	2022-01-12
F-Secure	Policy Manager	13-15		Affected	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
F-Secure	Policy Manager Proxy	13-15		Affected	link			cisagov	2022-01-12
F5	BIG-IP (all modules)			Not Affected	link			cisagov	2022-01-12
F5	BIG-IQ Centralized Management			Not Affected	link			cisagov	2022-01-12
F5	F5OS			Not Affected	link			cisagov	2022-01-12
F5	NGINX App Protect			Not Affected	link			cisagov	2022-01-12
F5	NGINX Controller			Not Affected	link			cisagov	2022-01-12
F5	NGINX Ingress Controller			Not Affected	link			cisagov	2022-01-12
F5	NGINX Instance Manager			Not Affected	link			cisagov	2022-01-12
F5	NGINX Open Source			Not Affected	link			cisagov	2022-01-12
F5	NGINX Plus			Not Affected	link			cisagov	2022-01-12
F5	NGINX Service Mesh			Not Affected	link			cisagov	2022-01-12
F5	NGINX Unit			Not Affected	link			cisagov	2022-01-12
F5	Traffix SDC	5.x (5.2.0 CF1, 5.1.0 CF-30 - 5.1.0 CF-33)		Affected	link	Vulnerable components: EMS-ELK components (Fluentd + Elastic Search + Kibana), Element Management System		cisagov	2022-01-12
FAST LTA				Unknown	link			cisagov	2022-01-12
Fastly				Unknown	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
FedEx	Ship Manager Software	Unknown		Affected	link	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.		cisagov	2021-12-15

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Fiix	Fiix CMMS Core		v5	Fixed	link	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.		cisagov	2021-12-15
	FileCap			Unknown	link			cisagov	2022-01-12
	FileCatalyst			Unknown	link			cisagov	2022-01-12
	FileCloud			Unknown	link			cisagov	2022-01-12
	FileWave			Unknown	link			cisagov	2022-01-12
	FINVI			Unknown	link			cisagov	2022-01-12
	FireDaemon			Unknown	link			cisagov	2022-01-12
	Fisher & Paykel Healthcare			Unknown	link			cisagov	2021-12-21
	Flexagon			Unknown	link			cisagov	2022-01-12
	Flexera			Unknown	link			cisagov	2022-01-12
	Forcepoint DLP Manager			Unknown	link			cisagov	2022-01-12
	Forcepoint Forcepoint Cloud Security Gateway (CSG)			Unknown	link			cisagov	2022-01-12
	Forcepoint Next Generation Firewall (NGFW)			Unknown	link			cisagov	2022-01-12
	Forcepoint Next Generation Firewall, NGFW VPN Client, Forcepoint User ID service and Sidewinder One			Unknown	link			cisagov	2022-01-12
	Forcepoint Endpoint Security Manager (Web, Email and DLP)			Unknown	link			cisagov	2022-01-12
	Forescout			Unknown	link			cisagov	2022-01-12
	ForgeRock Autonomous Identity			Unknown	link	all other ForgeRock products Not vulnerable		cisagov	2022-01-12
	Fortinet FortiAIops			Unknown	link			cisagov	2022-01-12
	Fortinet FortiAnalyzer			Unknown	link			cisagov	2022-01-12
	Fortinet FortiAnalyzer Cloud			Unknown	link			cisagov	2022-01-12
	Fortinet FortiAP			Unknown	link			cisagov	2022-01-12
	Fortinet FortiAuthenticator			Unknown	link			cisagov	2022-01-12
	Fortinet FortiCASB			Unknown	link			cisagov	2022-01-12
	Fortinet FortiConverto			Unknown	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Fortinet	FortiDeceptor			Unknown	link			cisagov	2022-01-12
Fortinet	FortiEDR Agent			Unknown	link			cisagov	2022-01-12
Fortinet	FortiEDR Cloud			Unknown	link			cisagov	2022-01-12
Fortinet	FortiGate Cloud			Unknown	link			cisagov	2022-01-12
Fortinet	FortiGSLB Cloud			Unknown	link			cisagov	2022-01-12
Fortinet	FortiMail			Unknown	link			cisagov	2022-01-12
Fortinet	FortiManager			Unknown	link			cisagov	2022-01-12
Fortinet	FortiManager Cloud			Unknown	link			cisagov	2022-01-12
Fortinet	FortiNAC			Unknown	link			cisagov	2022-01-12
Fortinet	FortiNAC			Unknown	link			cisagov	2022-01-12
Fortinet	FortiOS (includes FortiGate & FortiWiFi)			Unknown	link			cisagov	2022-01-12
Fortinet	FortiPhish Cloud			Unknown	link			cisagov	2022-01-12
Fortinet	FortiPolicy			Unknown	link			cisagov	2022-01-12
Fortinet	FortiPortal			Unknown	link			cisagov	2022-01-12
Fortinet	FortiRecorder			Unknown	link			cisagov	2022-01-12
Fortinet	FortiSIEM			Unknown	link			cisagov	2022-01-12
Fortinet	FortiSOAR			Unknown	link			cisagov	2022-01-12
Fortinet	FortiSwicth Cloud in FortiLANCloud			Unknown	link			cisagov	2022-01-12
Fortinet	FortiSwitch & FortiSwitchManager			Unknown	link			cisagov	2022-01-12
Fortinet	FortiToken Cloud			Unknown	link			cisagov	2022-01-12
Fortinet	FortiVoice			Unknown	link			cisagov	2022-01-12
Fortinet	FortiWeb Cloud			Unknown	link			cisagov	2022-01-12
Fortinet	ShieldX			Unknown	link			cisagov	2022-01-12
FTAPI				Unknown	link			cisagov	2022-01-12
Fujitsu				Unknown	link			cisagov	2022-01-12
FusionAuth	FusionAuth			Not Affected	link			cisagov	2022-01-12
GE Digital				Unknown	link	This advisory is available to customers only and has not been reviewed by CISA.		cisagov	2021-12-22
GE Digital Grid				Unknown	link	This advisory is available to customers only and has not been reviewed by CISA.		cisagov	2021-12-22
GE Gas Power	Asset Performance Management (APM)			Unknown	link	GE verifying workaround.		cisagov	2021-12-22



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
GE Gas Power	Baseline Security Center (BSC)			Unknown	link	Vulnerability to be fixed by vendor provided workaround. No user actions necessary. Contact GE for details.		cisagov	2021-12-22
GE Gas Power	Baseline Security Center (BSC) 2.0			Unknown	link	Vulnerability to be fixed by vendor provided workaround. No user actions necessary. Contact GE for details.		cisagov	2021-12-22
GE Gas Power	Control Server			Unknown	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.		cisagov	2021-12-22
GE Gas Power	Tag Mapping Service			Unknown	link	Vulnerability fixed. No user actions necessary. Updated to log4j 2.16		cisagov	2021-12-22
GE Healthcare				Unknown	link	This advisory is not available at the time of this review, due to maintence on the GE Healthcare website.		cisagov	2021-12-22
Gearset				Unknown	link			cisagov	2022-01-12
Genesys				Unknown	link			cisagov	2022-01-12
GeoServer				Unknown	link			cisagov	2022-01-12
Gerrit				Unknown	link			cisagov	2022-01-12
code review									
GFI				Unknown	link			cisagov	2022-01-12
Ghidra				Unknown	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Gigamon	Fabric Manager	<5.13.01.02		Affected	link	Updates available via the Gigamon Support Portal. This advisory available to customers only and has not been reviewed by CISA.		cisagov	2021-12-21
GitHub	GitHub		GitHub.com and GitHub Enterprise Cloud	Fixed	link			cisagov	2021-12-17
GitLab				Unknown	link			cisagov	2022-01-12
Globus				Unknown	link			cisagov	2022-01-12
GoAnywhere Gateway		< 2.8.4		Affected	link			cisagov	2021-12-18
GoAnywhere MFT		< 6.8.6		Affected	link			cisagov	2021-12-18
GoAnywhere MFT Agents		< 1.6.5		Affected	link			cisagov	2021-12-18
GoCD				Unknown	link			cisagov	2022-01-12
Google Cloud	Access Transparency			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Actifio			Unknown	link	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).		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	AI Platform Data Labeling			Unknown	<a href="#">link</a>	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	AI Platform Neural Architecture Search (NAS)			Unknown	<a href="#">link</a>	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	AI Platform Training and Prediction			Unknown	<a href="#">link</a>	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Anthos			Unknown	<a href="#">link</a>	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.		cisagov	2021-12-21
Google Cloud	Anthos Config Management			Unknown	<a href="#">link</a>	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Anthos Connect			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Anthos Hub			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Anthos Identity Service			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Anthos on VMWare			Unknown	link	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.		cisagov	2021-12-21
Google Cloud	Anthos Premium Software			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Anthos Service Mesh			Unknown	<a href="#">link</a>	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Apigee			Unknown	link	<p>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.</p>		cisagov	2021-12-17



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	App Engine			Unknown	<a href="#">link</a>	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.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	AppSheet			Unknown	link	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.		cisagov	2021-12-21
Google Cloud	Artifact Registry			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Assured Workloads			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	AutoML			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	AutoML Natural Language			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	AutoML Tables			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	AutoML Translation			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	AutoML Video			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	AutoML Vision			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	BigQuery			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	BigQuery Data Transfer Service			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	BigQuery Omni			Unknown	link	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.		cisagov	2021-12-19
Google Cloud	Binary Authorization			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Certificate Manager			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Chronicle			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-20
Google Cloud	Cloud Asset Inventory			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Cloud Bigtable			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-19

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Cloud Build			Unknown	link	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.		cisagov	2021-12-21
Google Cloud	Cloud CDN			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-20

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Cloud Composer			Unknown	link	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.		cisagov	2021-12-15



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Cloud Console App			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Cloud Data Loss Prevention			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Cloud Debugger			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Cloud Deployment Manager			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Cloud DNS			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-20
Google Cloud	Cloud Endpoints			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Cloud External Key Manager (EKM)			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Cloud Functions			Unknown	link	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.		cisagov	2021-12-21
Google Cloud	Cloud Hardware Security Module (HSM)			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Cloud Interconnect			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Cloud Intrusion Detection System (IDS)			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Cloud Key Management Service			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Cloud Load Balancing			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-20

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Cloud Logging			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Cloud Natural Language API			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Cloud Network Address Translation (NAT)			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-20
Google Cloud	Cloud Profiler			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Cloud Router			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-20
Google Cloud	Cloud Run			Unknown	link	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.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Cloud Run for Anthos			Unknown	link	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.		cisagov	2021-12-21
Google Cloud	Cloud Scheduler			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Cloud SDK			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Cloud Shell			Unknown	link	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.		cisagov	2021-12-21



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Cloud Source Repositories			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Cloud Spanner			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-19
Google Cloud	Cloud SQL			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-19
Google Cloud	Cloud Storage			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-20

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Cloud Tasks			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Cloud Trace			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Cloud Traffic Director			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-20
Google Cloud	Cloud Translation			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Cloud Vision			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Cloud Vision OCR On-Prem			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Cloud VPN			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-20
Google Cloud	CompilerWorks			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-20

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Compute Engine			Unknown	link	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.		cisagov	2021-12-20
Google Cloud	Contact Center AI (CCAI)			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Contact Center AI Insights			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Container Registry			Unknown	<a href="#">link</a>	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Data Catalog			Unknown	<a href="#">link</a>	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.		cisagov	2021-12-20

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Data Fusion			Unknown	link	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."		cisagov	2021-12-20
Google Cloud	Database Migration Service (DMS)			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-19

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Dataflow			Unknown	link	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.”		cisagov	2021-12-17

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Dataproc			Unknown	link	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.		cisagov	2021-12-20



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Dataproc Metastore			Unknown	link	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."		cisagov	2021-12-20
Google Cloud	Datastore			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-19
Google Cloud	Datastream			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-19

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Dialogflow Essentials (ES)			Unknown	<a href="#">link</a>	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Document AI			Unknown	<a href="#">link</a>	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Event Threat Detection			Unknown	<a href="#">link</a>	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Eventarc			Unknown	<a href="#">link</a>	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Filestore			Unknown	link	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.		cisagov	2021-12-21
Google Cloud	Firebase			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Firestore			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-19
Google Cloud	Game Servers			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Google Cloud Armor			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-20
Google Cloud	Google Cloud Armor Managed Protection Plus			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-20
Google Cloud	Google Cloud VMware Engine			Unknown	link	We are working with VMware and tracking VMSA-2021-0028.1. We will deploy fixes as they become available.		cisagov	2021-12-11

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Google Kubernetes Engine			Unknown	link	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.		cisagov	2021-12-21
Google Cloud	Healthcare Data Engine (HDE)			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Human-in-the-Loop AI			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	IoT Core			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Key Access Justifications (KAJ)			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Looker			Unknown	link	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.		cisagov	2021-12-18

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Media Translation API			Unknown	<a href="#">link</a>	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Memorystore			Unknown	<a href="#">link</a>	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-19
Google Cloud	Migrate for Anthos			Unknown	<a href="#">link</a>	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Migrate for Compute Engine (M4CE)			Unknown	link	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. Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-19
Google Cloud	Network Connectivity Center			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-20

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Network Intelligence Center			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-20
Google Cloud	Network Service Tiers			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-20
Google Cloud	Persistent Disk			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-20
Google Cloud	Pub/Sub			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-16

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Pub/Sub Lite			Unknown	link	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.		cisagov	2021-12-16
Google Cloud	reCAPTCHA Enterprise			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Recommendations AI			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Retail Search			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Risk Manager			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Secret Manager			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Security Command Center			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Service Directory			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Service Infrastructure			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Speaker ID			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Speech-to-Text			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Speech-to-Text On-Prem			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Storage Transfer Service			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-20
Google Cloud	Talent Solution			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Text-to-Speech			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Transcoder API			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Transfer Appliance			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Video Intelligence API			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Google Cloud	Virtual Private Cloud			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-20
Google Cloud	Web Security Scanner			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google Cloud	Workflows			Unknown	link	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		cisagov	2021-12-21
Google	Chrome			Not Affected	link	Chrome Browser releases, infrastructure and admin console are not using versions of Log4j affected by the vulnerability.		cisagov	2022-01-14
Gradle	Gradle			Unknown	link	Gradle Scala Compiler Plugin depends upon log4j-core but it is not used.		cisagov	2022-01-12
Gradle	Gradle Enterprise	< 2021.3.6		Affected	link			cisagov	2022-01-12



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Gradle	Gradle	< 10.1		Affected	link			cisagov	2022-01-12
	Enterprise Build Cache Node								
Gradle	Gradle Enterprise Test Distribution Agent	< 1.6.2		Affected	link			cisagov	2022-01-12
Grafana				Unknown	link			cisagov	2022-01-12
Grandstream				Unknown	link			cisagov	2022-01-12
Gravitee.io				Unknown	link			cisagov	2022-01-12
Gravitee	Access Management			Not Affected	link			cisagov	2022-01-12
Gravitee	Access Management			Not Affected	link			cisagov	2022-01-12
Gravitee	Alert Engine			Not Affected	link			cisagov	2022-01-12
Gravitee	Alert Engine			Not Affected	link			cisagov	2022-01-12
Gravitee	API Management			Not Affected	link			cisagov	2022-01-12
Gravitee	API Management			Not Affected	link			cisagov	2022-01-12
Gravitee	Cockpit			Not Affected	link			cisagov	2022-01-12
Gravwell				Unknown	link			cisagov	2022-01-12
Graylog	Graylog Server	All versions >= 1.2.0 and <= 4.2.2		Affected	link			cisagov	2022-01-12
GreenShot				Unknown	link			cisagov	2022-01-12
GSA	Cloud.gov			Unknown	link			cisagov	2021-12-21
Guidewire				Unknown	link			cisagov	2022-01-12
HAProxy				Unknown	link			cisagov	2022-01-12
HarmanPro				Unknown	link			cisagov	2022-01-12
AMX									
HashiCorp	Boundary			Unknown	link			cisagov	2022-01-12
HashiCorp	Consul			Unknown	link			cisagov	2022-01-12
HashiCorp	Consul Enterprise			Unknown	link			cisagov	2022-01-12
HashiCorp	Nomad			Unknown	link			cisagov	2022-01-12
HashiCorp	Nomad Enterprise			Unknown	link			cisagov	2022-01-12
HashiCorp	Packer			Unknown	link			cisagov	2022-01-12
HashiCorp	Terraform			Unknown	link			cisagov	2022-01-12
HashiCorp	Terraform Enterprise			Unknown	link			cisagov	2022-01-12
HashiCorp	Vagrant			Unknown	link			cisagov	2022-01-12
HashiCorp	Vault			Unknown	link			cisagov	2022-01-12
HashiCorp	Vault Enterprise			Unknown	link			cisagov	2022-01-12
HashiCorp	Waypoint			Unknown	link			cisagov	2022-01-12
HCL	BigFix			Not Affected	link			cisagov	2021-12-15
Software	Compliance					Not Affected for related CVE-2021-45046			
HCL	BigFix			Not Affected	link			cisagov	2021-12-15
Software	Insights					Not Affected for related CVE-2021-45046			
HCL	BigFix			Not Affected	link			cisagov	2021-12-15
Software	Insights for Vulnerability Remediation					Not Affected for related CVE-2021-45046			

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
HCL Software	BigFix Inventory		< 10.0.7	Fixed	link	Not Affected for related CVE-2021-45046		cisagov	2021-12-15
HCL Software	BigFix Lifecycle			Not Affected	link	Not Affected for related CVE-2021-45046		cisagov	2021-12-15
HCL Software	BigFix Mobile			Not Affected	link	Not Affected for related CVE-2021-45046		cisagov	2021-12-15
HCL Software	BigFix Patch			Not Affected	link	Not Affected for related CVE-2021-45046		cisagov	2021-12-15
HelpSystems Clearswift				Unknown	link			cisagov	2022-01-12
HENIX	Squash TM		1.21.7-1.22.9, 2.0.3-2.1.5, 2.2.0-3.0.2	Fixed	link			cisagov	2021-12-23
Hexagon Hikvision				Unknown	link			cisagov	2022-01-12
Hitachi Energy	3rd party - Elastic Search, Kibana		Elasticsearch 5.0.0+	Fixed	link	Set the JVM option - Dlog4j2.formatMsgNoLookups=true and restart each node of the cluster.		cisagov	2022-01-05
Hitachi Energy	3rd party - Oracle Database Components		12.1, 12.2, 19c	Fixed	link	As this is a third-party component, a separate patch management report will be provided to customers with the steps to apply the Oracle provided patches for these components.		cisagov	2022-01-05

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Hitachi Energy	Axis		3.6	Fixed	<a href="#">link</a>	No action is required by customers. Axis is a fully SaaS hosted solution and the environment has been patched per the recommendations		cisagov	2022-01-05
Hitachi Energy	Counterparty Settlement and Billing (CSB)		v6	Fixed	<a href="#">link</a>			cisagov	2022-01-05
Hitachi Energy	e-Mesh Monitor			Unknown	<a href="#">link</a>	No end-user action needed. The affected e-Mesh Monitor part is at the cloud offering side of which the remediation is handled by Hitachi Energy team. Remediation is currently ongoing, and during this time period, e-Mesh Monitor edge device is not able to upload data to cloud.		cisagov	2022-01-05
Hitachi Energy	eSOMS			Unknown	<a href="#">link</a>			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Hitachi Energy	FOXMAN-UN		R15A, R14B, R14A, R11B SP1	Fixed	<a href="#">link</a>	A patch is available for releases R15A, R14B, R14A and R11B SP1. . For details on how to apply such patch, please refer to the technical bulletin “FOXMAN-UN - Installation of Log4j Patch”, version A (1KHW029176) available in the Hitachi Energy Customer Connect Portal.		cisagov	2022-01-05
Hitachi Energy	FOXMAN-UN		R11A and R10 series	Fixed	<a href="#">link</a>	Apply General Mitigations and upgrade to latest version. For upgrades, please get in touch with your Hitachi Energy contacts.		cisagov	2022-01-05
Hitachi Energy	Lumada APM On-premises			Unknown	<a href="#">link</a>	See vendor advisory for instructions for various versions.		cisagov	2022-01-05
Hitachi Energy	Lumada APM SaaS offering			Unknown	<a href="#">link</a>	No action is required by customers. The SaaS offering has been patched per the recommendations.		cisagov	2022-01-05
Hitachi Energy	Lumada EAM / FSM		v1.7.x, v1.8.x, v1.9.x	Fixed	<a href="#">link</a>	See Section Mitigation Strategy in vendor advisory.		cisagov	2022-01-05

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Hitachi Energy	MMS Internal facing subcomponent.			Unknown	link			cisagov	2022-01-05
Hitachi Energy	Network Manager ADMS Network Model Server		9.1.0.32-9.1.0.44	Fixed	link	See vendor advisory for instructions on mitigation steps.		cisagov	2022-01-05
Hitachi Energy	Network Manager Outage Management Interface (CMI)		9.0-9.10.44, 9.1.1, 10.3.4	Fixed	link	See vendor advisory for instructions on mitigation steps.		cisagov	2022-01-05
Hitachi Energy	nMarket Global I-SEM		3.7.15, 3.7.16	Fixed	link			cisagov	2022-01-05
Hitachi Energy	RelCare		2.0.0	Fixed	link	No action is required by customers. The RelCare SaaS hosted solution and the on-premises have been patched per the recommendations.		cisagov	2022-01-05
Hitachi Energy	UNEM		R15A, R14B, R14A, R11B SP1	Fixed	link	A patch is available for releases R15A, R14B, R14A and R11B SP1. For details on how to apply such patch, please refer to the technical bulletin “UNEM - Installation of Log4j Patch”, version A (1KHW029176) available in the Hitachi Energy Customer Connect Portal.		cisagov	2022-01-05

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Hitachi Energy	UNEM		R11A and R10 series	Fixed	<a href="#">link</a>	Apply General Mitiga-tions and upgrade to latest version. For upgrades, please get in touch with your Hitachi Energy contacts.		cisagov	2022-01-05
Hitachi Vantara				Unknown	<a href="#">link</a>			cisagov	2022-01-12
HMS Industrial Networks AB	Cosy, Flexy and Ewon CD			Unknown	<a href="#">link</a>			cisagov	2022-01-05
HMS Industrial Networks AB	eCatcher Mobile applications			Unknown	<a href="#">link</a>			cisagov	2022-01-05
HMS Industrial Networks AB	eCatcher Windows software			Unknown	<a href="#">link</a>			cisagov	2022-01-05
HMS Industrial Networks AB	Netbiter Hardware including EC, WS, and LC			Unknown	<a href="#">link</a>			cisagov	2022-01-05
HMS Industrial Networks AB	Talk2M including M2Web			Unknown	<a href="#">link</a>			cisagov	2022-01-05
HOLOGIC AB	Advanced Workflow Manager (AWM)			Unknown	<a href="#">link</a>	While the Hologic software itself does not utilize Java/Log4J, the installed APC Pow-erChute UPS with Business Edition v9.5 software installed may. APC is still assessing its Power-Chute software to deter-mine if it is vulnerable.		cisagov	2021-12-20
HOLOGIC	Affirm Prone Biopsy System			Unknown	<a href="#">link</a>			cisagov	2021-12-20

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
HOLOGIC	Brevera Breast Biopsy System			Unknown	link			cisagov	2021-12-20
HOLOGIC	Cenova Image Analytics Server			Unknown	link			cisagov	2021-12-20
HOLOGIC	Dimensions / 3Dimensions Mammography System			Unknown	link			cisagov	2021-12-20
HOLOGIC	Discovery Bone Densitometer			Unknown	link			cisagov	2021-12-20
HOLOGIC	Faxitron CT Specimen Radiography System			Unknown	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.		cisagov	2021-12-20
HOLOGIC	Faxitron Specimen Radiography Systems			Unknown	link			cisagov	2021-12-20
HOLOGIC	Fluoroscanner Insight Mini C-Arm			Unknown	link			cisagov	2021-12-20
HOLOGIC	Horizon DXA Bone Densitometer			Unknown	link			cisagov	2021-12-20
HOLOGIC	Rosetta DC Tomosynthesis Data Converter			Unknown	link			cisagov	2021-12-20
HOLOGIC	SecurView DX Workstation			Unknown	link			cisagov	2021-12-20
HOLOGIC	SecurXChange Router			Unknown	link			cisagov	2021-12-20

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
HOLOGIC	SuperSonic Imagine Ultrasound Products (Aixplorer & Aixplorer Mach)			Unknown	link			cisagov	2021-12-20
HOLOGIC	Trident HD Specimen Radiography System			Unknown	link			cisagov	2021-12-20
HOLOGIC	Unifi Workspace			Unknown	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.		cisagov	2021-12-20
HOLOGIC	Windows Selenia Mammography System			Unknown	link			cisagov	2021-12-20
Honeywell HPE/Micro Focus	Data Protector		9.09	Unknown Fixed	link link		https://portal.microfocus.com/s/article/KM000003050	cisagov cisagov	2022-01-12 2021-12-17
HPE	3PAR StoreServ Arrays			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	AirWave Management Platform			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Alletra 6000			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
HPE	Alletra 9k			Unknown	link	Support Communi- cation Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Aruba Central			Unknown	link	Support Communi- cation Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Aruba ClearPass Policy Manager			Unknown	link	Support Communi- cation Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Aruba ClearPass Policy Manager			Unknown	link	Support Communi- cation Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Aruba Instant (IAP)			Unknown	link	Support Communi- cation Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Aruba Location Services			Unknown	link	Support Communi- cation Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Aruba NetEdit			Unknown	link	Support Communi- cation Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Aruba PVOS Switches			Unknown	link	Support Communi- cation Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Aruba SDN VAN Controller			Unknown	link	Support Communi- cation Cross Reference ID: SIK7387		cisagov	2021-12-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
HPE	Aruba User Experience Insight (UXI)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Aruba VIA Client			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	ArubaOS SD-WAN Controllers and Gateways			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	ArubaOS Wi-Fi Controllers and Gateways			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	ArubaOS-CX switches			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	ArubaOS-S switches			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	BladeSystem Onboard Administrator			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Brocade 16Gb Fibre Channel SAN Switch for HPE Synergy			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Brocade 16Gb SAN Switch for HPE BladeSystem c-Class			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
HPE	Brocade 32Gb Fibre Channel SAN Switch for HPE Synergy			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Brocade Network Advisor			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	CloudAuth			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	CloudPhysics			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Compute Cloud Console			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Compute operations manager- FW UPDATE SERVICE			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	COS (Cray Operating System)			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Cray Systems Management (CSM)			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Custom SPP Portal Link			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
HPE	Data Services Cloud Console			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Harmony Data Platform			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HOP public services (grafana, vault, rancher, Jenkins)			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HPE B-series SN2600B SAN Extension Switch			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HPE B-series SN4000B SAN Extension Switch			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HPE B-series SN6000B Fibre Channel Switch			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HPE B-series SN6500B Fibre Channel Switch			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HPE B-series SN6600B Fibre Channel Switch			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HPE B-series SN6650B Fibre Channel Switch			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
HPE	HPE B-series SN6700B Fibre Channel Switch			Unknown	<a href="#">link</a>	Support Communi- cation Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HPE Customer Experience Assurance (CEA)			Unknown	<a href="#">link</a>	Support Communi- cation Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE Hardware Support Manager plug-in for VMware vSphere Lifecycle Manager			Unknown	<a href="#">link</a>	Support Communi- cation Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HPE Home Location Register (HLR/I- HLR)			Unknown	<a href="#">link</a>	Support Communi- cation Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE Infosight for Servers			Unknown	<a href="#">link</a>	Support Communi- cation Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HPE Integrated Home Subscriber Server (I-HSS)			Unknown	<a href="#">link</a>	Support Communi- cation Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE Intelligent Messaging (IM)			Unknown	<a href="#">link</a>	Support Communi- cation Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE Intelligent Network Server (INS)			Unknown	<a href="#">link</a>	Support Communi- cation Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE Multimedia Services Environment (MSE)			Unknown	<a href="#">link</a>	Support Communi- cation Cross Reference ID: SIK7387		cisagov	2021-12-14

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
HPE	HPE OC Convergent Communications Platform (OCCP)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE OC Media Platform Media Resource Function (OCMP-MRF)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE OC Service Access Controller (OC SAC)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE OC Service Controller (OCSC)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE OC Universal Signaling Platform (OC-USP-M)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE OneView			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HPE OneView for VMware vRealize Operations (vROps)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HPE OneView Global Dashboard			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HPE Performance Cluster Manager (HPCM)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
HPE	HPE Performance Manager (PM)			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE Position Determination Entity (PDE)			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE Secure Identity Broker (SIB)			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE Service Activator (SA)			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE Service Governance Framework (SGF)			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE Service Orchestration Manager (SOM)			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE Service Provisioner (SP)			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE Short Message Point-to-Point Gateway (SMPP)			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE Slingshot			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
HPE	HPE Smart Interaction Server (SIS)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE SN3000B Fibre Channel Switch			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HPE SN8000B 4-Slot SAN Director Switch			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HPE SN8000B 8-Slot SAN Backbone Director Switch			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HPE SN8600B 4-Slot SAN Director Switch			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HPE SN8600B 8-Slot SAN Director Switch			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HPE SN8700B 4-Slot Director Switch			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HPE SN8700B 8-Slot Director Switch			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HPE Subscriber, Network, and Application Policy (SNAP)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
HPE	HPE Subscription Manager (SM)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE Synergy Image Streamer			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HPE Systems Insight Manager (SIM)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HPE Telecom Application Server (TAS)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE Unified Correlation and Automation (UCA)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE Unified Mediation Bus (UMB)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE Unified OSS Console (UOC)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE Unified Topology Manager (UTM)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE Universal Identity Repository (VIR)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
HPE	HPE Universal SLA Manager (uSLAM)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE Virtual Connect			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HPE Virtual Connect Enterprise Manager (VCEM)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HPE Virtual Provisioning Gateway (vPGW)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE Virtual Server Environment (VSE)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	HPE Virtual Subscriber Data Management (vSDM)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE WebRTC Gateway Controller (WGW)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-14
HPE	HPE Wi-Fi Authentication Gateway (WauG)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Insight Cluster Management Utility (CMU)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
HPE	Integrated Lights-Out (iLO) Amplifier Pack			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Integrated Lights-Out 4 (iLO 4)			Not Affected	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Integrated Lights-Out 5 (iLO 5)			Not Affected	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Integrity BL860c, BL870c, BL890c			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Integrity Rx2800/Rx2900			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Integrity Superdome 2			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Integrity Superdome X			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Intelligent Provisioning			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	iSUT integrated smart update tool			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
HPE	Maven Artifacts (Atlas)			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	MSA			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	NetEdit			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Nimble Storage			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	NS-T0634-OSM CONSOLE TOOLS			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	NS-T0977-SCHEMA VALIDATOR			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	OfficeConnect			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Primera Storage			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	RepoServer part of OPA (on Premises aggregator)			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
HPE	Resource Aggregator for Open Distributed Infrastructure Management			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	RESTful Interface Tool (iLOREST)			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	SAT (System Admin Toolkit)			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Scripting Tools for Windows PowerShell (HPEiLOCmdlets)			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	SGI MC990 X Server			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	SGI UV 2000 Server			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	SGI UV 300, 300H, 300RL, 30EX			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	SGI UV 3000 Server			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	SN8700B 8-Slot Director Switch			Unknown	link	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
HPE	StoreEasy			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	StoreEver CVTL			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	StoreEver LTO Tape Drives			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	StoreEver MSL Tape Libraries			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	StoreOnce			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	SUM (Smart Update Manager)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Superdome Flex 280			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	Superdome Flex Server			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HPE	UAN (User Access Node)			Unknown	<a href="#">link</a>	Support Communication Cross Reference ID: SIK7387		cisagov	2021-12-12
HP	Teradici Cloud Access Controller		< v113	Fixed	<a href="#">link</a>	SIK7387		cisagov	2021-12-17
HP	Teradici EMSDK		< 1.0.6	Fixed	<a href="#">link</a>			cisagov	2021-12-17

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
HP	Teradici Management Console		< 21.10.3	Fixed	link			cisagov	2021-12-17
HP	Teradici PCoIP Connection Manager		< 21.03.6, < 20.07.4	Fixed	link			cisagov	2021-12-17
HP	Teradici PCoIP License Server			Unknown	link			cisagov	2021-12-17
Huawei Hubspot				Unknown	link			cisagov	2022-01-12
I-Net software				Unknown	link			cisagov	2022-01-12
I2P				Unknown	link			cisagov	2022-01-12
IBA-AG				Unknown	link			cisagov	2022-01-12
Ibexa				Unknown	link			cisagov	2022-01-12
IBM	Analytics Engine			Unknown	link			cisagov	2021-12-15
IBM	App Configuration			Unknown	link			cisagov	2021-12-15
IBM	App Connect			Unknown	link			cisagov	2021-12-15
IBM	App ID			Unknown	link			cisagov	2021-12-15
IBM	Application Gateway			Unknown	link			cisagov	2021-12-15
IBM	Aspera			Unknown	link			cisagov	2021-12-15
IBM	Aspera			Unknown	link			cisagov	2021-12-15
IBM	Endpoint			Unknown	link			cisagov	2021-12-15
IBM	Aspera Enterprise			Unknown	link			cisagov	2021-12-15
IBM	fasp.io			Unknown	link			cisagov	2021-12-15
IBM	Bare Metal Servers			Unknown	link			cisagov	2021-12-15
IBM	BigFix Compliance			Unknown				cisagov	2022-01-12
IBM	BigFix Inventory	VM Manager Tool & SAP Tool		Affected		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.		cisagov	2022-01-12
IBM	Block Storage			Unknown	link			cisagov	2021-12-15
IBM	Block Storage for VPC			Unknown	link			cisagov	2021-12-15
IBM	Block Storage Snapshots for VPC			Unknown	link			cisagov	2021-12-15

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
IBM	Case Manager			Unknown	link			cisagov	2021-12-15
IBM	Certificate Manager			Unknown	link			cisagov	2021-12-15
IBM	Client VPN for VPC			Unknown	link			cisagov	2021-12-15
IBM	Cloud Activity Tracker			Unknown	link			cisagov	2021-12-15
IBM	Cloud Backup			Unknown	link			cisagov	2021-12-15
IBM	Cloud Monitoring			Unknown	link			cisagov	2021-12-15
IBM	Cloud Object Storage			Unknown	link			cisagov	2021-12-15
IBM	Cloud Object Storage			Unknown	link			cisagov	2021-12-15
IBM	Cloudant			Unknown	link			cisagov	2021-12-15
IBM	Code Engine			Unknown	link			cisagov	2021-12-15
IBM	Cognos Command Center			Unknown	link			cisagov	2021-12-15
IBM	Cognos Controller	10.4.2		Affected	link			cisagov	2021-12-15
IBM	Cognos Integration Server			Unknown	link			cisagov	2021-12-15
IBM	Compose Enterprise			Unknown	link			cisagov	2021-12-15
IBM	Compose for Elasticsearch			Unknown	link			cisagov	2021-12-15
IBM	Compose for etcd			Unknown	link			cisagov	2021-12-15
IBM	Compose for MongoDB			Unknown	link			cisagov	2021-12-15
IBM	Compose for MySQL			Unknown	link			cisagov	2021-12-15
IBM	Compose for PostgreSQL			Unknown	link			cisagov	2021-12-15
IBM	Compose for RabbitMQ			Unknown	link			cisagov	2021-12-15
IBM	Compose for Redis			Unknown	link			cisagov	2021-12-15
IBM	Compose for RethinkDB			Unknown	link			cisagov	2021-12-15
IBM	Compose for ScyllaDB			Unknown	link			cisagov	2021-12-15
IBM	Container Registry			Unknown	link			cisagov	2021-12-15
IBM	Container Security Services			Unknown	link			cisagov	2021-12-15
IBM	Content Delivery Network			Unknown	link			cisagov	2021-12-15
IBM	Continuous Delivery			Unknown	link			cisagov	2021-12-15
IBM	Copy Services Manager			Unknown	link			cisagov	2021-12-15
IBM	Databases for DataStax			Unknown	link			cisagov	2021-12-15
IBM	Databases for EDB			Unknown	link			cisagov	2021-12-15
IBM	Databases for Elasticsearch			Unknown	link			cisagov	2021-12-15
IBM	Databases for etcd			Unknown	link			cisagov	2021-12-15



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
IBM	Databases for MongoDB			Unknown	link			cisagov	2021-12-15
IBM	Databases for PostgreSQL			Unknown	link			cisagov	2021-12-15
IBM	Databases for Redis			Unknown	link			cisagov	2021-12-15
IBM	Datapower Gateway			Unknown	link			cisagov	2021-12-15
IBM	Dedicated Host for VPC			Unknown	link			cisagov	2021-12-15
IBM	Direct Link Connect			Unknown	link			cisagov	2021-12-15
IBM	Direct Link Connect on Classic			Unknown	link			cisagov	2021-12-15
IBM	Direct Link Dedicated (2.0)			Unknown	link			cisagov	2021-12-15
IBM	Direct Link Dedicated Hosting on Classic			Unknown	link			cisagov	2021-12-15
IBM	Direct Link Dedicated on Classic			Unknown	link			cisagov	2021-12-15
IBM	Direct Link Exchange on Classic			Unknown	link			cisagov	2021-12-15
IBM	DNS Services			Unknown	link			cisagov	2021-12-15
IBM	Emptoris Contract Management			Unknown	link			cisagov	2021-12-15
IBM	Emptoris Program Management			Unknown	link			cisagov	2021-12-15
IBM	Emptoris Sourcing			Unknown	link			cisagov	2021-12-15
IBM	Emptoris Spend Analysis			Unknown	link			cisagov	2021-12-15
IBM	Emptoris Supplier Lifecycle Management			Unknown	link			cisagov	2021-12-15
IBM	Enterprise Tape Controller Model C07 (3592) (ETC)			Unknown	link			cisagov	2021-12-15
IBM	Event Notifications			Unknown	link			cisagov	2021-12-15
IBM	Event Streams			Unknown	link			cisagov	2021-12-15
IBM	File Storage			Unknown	link			cisagov	2021-12-15
IBM	Flash System 900 (& 840)			Unknown	link			cisagov	2021-12-15
IBM	Flow Logs for VPC			Unknown	link			cisagov	2021-12-15
IBM	Functions			Unknown	link			cisagov	2021-12-15
IBM	GSKit			Unknown	link			cisagov	2021-12-15
IBM	Guardium S-TAP for Data Sets on z/OS			Unknown	link			cisagov	2021-12-15
IBM	Guardium S-TAP for DB2 on z/OS			Unknown	link			cisagov	2021-12-15

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
IBM	Guardium S-TAP for IMS on z/OS			Unknown	link			cisagov	2021-12-15
IBM	Hyper Protect Crypto Services			Unknown	link			cisagov	2021-12-15
IBM	Hyper Protect DBaaS for MongoDB			Unknown	link			cisagov	2021-12-15
IBM	Hyper Protect DBaaS for PostgreSQL			Unknown	link			cisagov	2021-12-15
IBM	Hyper Protect Virtual Server			Unknown	link			cisagov	2021-12-15
IBM	i2 Analyst's Notebook			Unknown	link			cisagov	2021-12-15
IBM	i2 Base			Unknown	link			cisagov	2021-12-15
IBM	Application Runtime Expert for i			Unknown	link			cisagov	2021-12-15
IBM	IBM Backup, Recovery and Media Services for i			Unknown	link			cisagov	2021-12-15
IBM	IBM Db2 Mirror for i			Unknown	link			cisagov	2021-12-15
IBM	IBM HTTP Server			Unknown	link			cisagov	2021-12-15
IBM	IBM i Access Family			Unknown	link			cisagov	2021-12-15
IBM	IBM i Portfolio of products under the Group			Unknown	link			cisagov	2021-12-15
IBM	SWMA IBM PowerHA System Mirror for i			Unknown	link			cisagov	2021-12-15
IBM	IBM Sterling Con-nect:Direct Browser User Interface			Unknown	link			cisagov	2021-12-15
IBM	IBM Sterling Con-nect:Direct File Agent	See Vendor Links		Affected	link		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/	cisagov	2021-12-20

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
IBM	IBM Sterling Connect:Direct for HP NonStop	Timestamp lower than 12-11-2021		Unknown	link			cisagov	2021-12-15
IBM	IBM Sterling Connect:Direct for i5/OS			Unknown	link			cisagov	2021-12-15
IBM	IBM Sterling Connect:Direct for OpenVMS			Unknown	link			cisagov	2021-12-15
IBM	IBM Sterling Connect:Express for Microsoft Windows			Unknown	link			cisagov	2021-12-15
IBM	IBM Sterling Connect:Express for UNIX			Unknown	link			cisagov	2021-12-15
IBM	IBM Sterling Connect:Express for z/OS			Unknown	link			cisagov	2021-12-15
IBM	Instana Agent			Affected	link			cisagov	2021-12-14
IBM	Internet Services			Unknown	link			cisagov	2021-12-15
IBM	Key Lifecycle Manager for z/OS			Unknown	link			cisagov	2021-12-15
IBM	Key Protect			Unknown	link			cisagov	2021-12-15
IBM	Knowledge Studio			Unknown	link			cisagov	2021-12-15
IBM	Kubernetes Service			Unknown	link			cisagov	2021-12-15
IBM	Load Balancer for VPC			Unknown	link			cisagov	2021-12-15
IBM	Log Analysis			Unknown	link			cisagov	2021-12-15
IBM	Managed VMware Service			Unknown	link			cisagov	2021-12-15
IBM	Management Extender for VMware vCenter			Unknown				cisagov	2022-01-12
IBM	Mass Data Migration			Unknown	link			cisagov	2021-12-15
IBM	Maximo EAM SaaS			Unknown	link			cisagov	2021-12-15
IBM	Message Hub			Unknown	link			cisagov	2021-12-15
IBM	MQ Appliance			Unknown	link			cisagov	2021-12-15
IBM	MQ on IBM Cloud			Unknown	link			cisagov	2021-12-15
IBM	Natural Language Understanding			Unknown	link			cisagov	2021-12-15
IBM	OmniFind Text Search Server for DB2 for i			Unknown	link			cisagov	2021-12-15
IBM	OPENBMC			Unknown	link			cisagov	2021-12-15

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
IBM	Planning Analytics Workspace	>2.0.57		Affected	link			cisagov	2021-12-15
IBM	Power HMC	V9.2.950.0 & V10.1.1010.0		Affected	link			cisagov	2021-12-15
IBM	PowerSC			Unknown	link			cisagov	2021-12-15
IBM	PowerVM Hypervisor			Unknown	link			cisagov	2021-12-15
IBM	PowerVM VIOS			Unknown	link			cisagov	2021-12-15
IBM	QRadar Advisor			Unknown	link			cisagov	2021-12-15
IBM	QRadar Network Threat Analytics			Unknown	link			cisagov	2021-12-15
IBM	QRadar SIEM			Unknown	link			cisagov	2021-12-15
IBM	Quantum Services			Unknown	link			cisagov	2021-12-15
IBM	Rational Developer for AIX and Linux			Unknown	link			cisagov	2021-12-15
IBM	Rational Developer for i			Unknown	link			cisagov	2021-12-15
IBM	Red Hat OpenShift on IBM Cloud			Unknown	link			cisagov	2021-12-15
IBM	Resilient			Unknown				cisagov	2022-01-12
IBM	Robotic Process Automation			Unknown	link			cisagov	2021-12-15
IBM	SAN Volume Controller and Storwize Family			Unknown	link			cisagov	2021-12-15
IBM	Satellite Infrastructure Service			Unknown	link			cisagov	2021-12-15
IBM	Schematics			Unknown	link			cisagov	2021-12-15
IBM	Secrets Manager			Unknown	link			cisagov	2021-12-15
IBM	Secure Gateway Server			Unknown				cisagov	2022-01-12
IBM	Automation Spectrum Archive Library Edition			Unknown	link			cisagov	2021-12-15
IBM	Spectrum Discover			Unknown	link			cisagov	2021-12-15
IBM	Spectrum Protect Client Management Service			Unknown	link			cisagov	2021-12-15
IBM	Spectrum Protect for Databases: Data Protection for Oracle			Unknown	link			cisagov	2021-12-15

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
IBM	Spectrum Protect for Databases: Data Protection for SQL			Unknown	link			cisagov	2021-12-15
IBM	Spectrum Protect for Enterprise Resource Planning			Unknown	link			cisagov	2021-12-15
IBM	Spectrum Protect for Mail: Data Protection for Domino			Unknown	link			cisagov	2021-12-15
IBM	Spectrum Protect for Mail: Data Protection for Exchange			Unknown	link			cisagov	2021-12-15
IBM	Spectrum Protect for Workstations			Unknown	link			cisagov	2021-12-15
IBM	Spectrum Protect for z/OS USS Client and API			Unknown	link			cisagov	2021-12-15
IBM	Spectrum Protect Plus Db2 Agent			Unknown	link			cisagov	2021-12-15
IBM	Spectrum Protect Plus Exchange Agent			Unknown	link			cisagov	2021-12-15
IBM	Spectrum Protect Plus File Systems Agent			Unknown	link			cisagov	2021-12-15
IBM	Spectrum Protect Plus MongoDB Agent			Unknown	link			cisagov	2021-12-15
IBM	Spectrum Protect Plus O365 Agent			Unknown	link			cisagov	2021-12-15
IBM	Spectrum Protect Server			Unknown	link			cisagov	2021-12-15
IBM	Spectrum Protect Snapshot for UNIX			Unknown	link			cisagov	2021-12-15
IBM	Spectrum SQL Query			Unknown	link			cisagov	2021-12-15
IBM	Sterling Gentran			Unknown	link			cisagov	2021-12-15
IBM	Sterling Order Management			Unknown	link			cisagov	2021-12-15

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
IBM	Sterling Transformation Extender Pack for ACORD			Unknown	link			cisagov	2021-12-15
IBM	Sterling Transformation Extender Pack for Financial Services			Unknown	link			cisagov	2021-12-15
IBM	Sterling Transformation Extender Pack for FIX			Unknown	link			cisagov	2021-12-15
IBM	Sterling Transformation Extender Pack for NACHA			Unknown	link			cisagov	2021-12-15
IBM	Sterling Transformation Extender Pack for PeopleSoft			Unknown	link			cisagov	2021-12-15
IBM	Sterling Transformation Extender Pack for SAP R/3			Unknown	link			cisagov	2021-12-15
IBM	Sterling Transformation Extender Pack for SEPA			Unknown	link			cisagov	2021-12-15
IBM	Sterling Transformation Extender Pack for Siebel			Unknown	link			cisagov	2021-12-15
IBM	Sterling Transformation Extender Packs for SWIFT			Unknown	link			cisagov	2021-12-15
IBM	Sterling Transformation Extender Packs for EDI			Unknown	link			cisagov	2021-12-15
IBM	Sterling Transformation Extender Packs for Healthcare			Unknown	link			cisagov	2021-12-15
IBM	Sterling Transformation Extender Trading Manager			Unknown	link			cisagov	2021-12-15
IBM	Storage TS1160			Unknown	link			cisagov	2021-12-15
IBM	Storage TS2280			Unknown	link			cisagov	2021-12-15
IBM	Storage TS2900 Library			Unknown	link			cisagov	2021-12-15

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
IBM	Storage TS3100-TS3200 Library			Unknown	link			cisagov	2021-12-15
IBM	Storage TS4500 Library			Unknown	link			cisagov	2021-12-15
IBM	Storage Virtualization Engine TS7700			Unknown	link			cisagov	2021-12-15
IBM	Tape System Library Manager			Unknown	link			cisagov	2021-12-15
IBM	TDMF for zOS			Unknown	link			cisagov	2021-12-15
IBM	Total Storage Service Console (TSSC) / TS4500 IMC			Unknown	link			cisagov	2021-12-15
IBM	Transit Gateway			Unknown	link			cisagov	2021-12-15
IBM	Tririga Anywhere			Unknown	link			cisagov	2021-12-15
IBM	TS4300			Unknown	link			cisagov	2021-12-15
IBM	Urbancode Deploy			Unknown	link			cisagov	2021-12-15
IBM	Virtual Private Cloud			Unknown	link			cisagov	2021-12-15
IBM	Virtual Server for Classic			Unknown	link			cisagov	2021-12-15
IBM	Virtualization Management Interface			Unknown	link			cisagov	2021-12-15
IBM	VMware Solutions			Unknown	link			cisagov	2021-12-15
IBM	VMware vCenter Server			Unknown	link			cisagov	2021-12-15
IBM	VMware vSphere			Unknown	link			cisagov	2021-12-15
IBM	VPN for VPC			Unknown	link			cisagov	2021-12-15
IBM	vRealize Operations and Log Insight			Unknown	link			cisagov	2021-12-15
IBM	Workload Automation			Unknown	link			cisagov	2021-12-15
ICONICS	All			Unknown	link			cisagov	2021-12-21
IFS				Unknown	link			cisagov	2022-01-12
IGEL				Unknown	link			cisagov	2022-01-12
Ignite				Unknown	link			cisagov	2022-01-12
Realtime				Unknown	link			cisagov	2022-01-12
iGrafx				Unknown	link			cisagov	2022-01-12
Illuminated				Unknown	link			cisagov	2022-01-12
Cloud				Unknown	link			cisagov	2021-12-16
Illumio	C-VEN			Unknown	link			cisagov	2021-12-16
Illumio	CLI			Unknown	link			cisagov	2021-12-16
Illumio	CloudSecure			Unknown	link			cisagov	2021-12-16
Illumio	Core on-premise			Unknown	link			cisagov	2021-12-16
	PCE								
Illumio	Core SaaS			Unknown	link			cisagov	2021-12-16
	PCE								

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Illumio	Edge SaaS			Unknown	link			cisagov	2021-12-16
Illumio	PCE			Unknown	link			cisagov	2021-12-16
Illumio	Edge-CrowdStrike			Unknown	link			cisagov	2021-12-16
Illumio	Flowlink			Unknown	link			cisagov	2021-12-16
Illumio	Kubelink			Unknown	link			cisagov	2021-12-16
Illumio	NEN			Unknown	link			cisagov	2021-12-16
Illumio	QRadar App			Unknown	link			cisagov	2021-12-16
Illumio	Splunk App			Unknown	link			cisagov	2021-12-16
Illumio	VEN			Unknown	link			cisagov	2021-12-16
IManage				Unknown	link			cisagov	2022-01-12
Imperva				Unknown	link			cisagov	2022-01-12
Inductive Automation	Ignition			Not Affected	link	Older versions of Ignition (7.8 and older) did use the Log4j library, but they used an older version (1.2) that was not affected by this vulnerability.		cisagov	2022-01-19
IndustrialDefender				Unknown	link			cisagov	2022-01-12
infinidat				Unknown	link			cisagov	2022-01-12
InfluxData				Unknown	link			cisagov	2022-01-12
Infoblox				Unknown	link			cisagov	2022-01-12
Informatica				Unknown	link			cisagov	2022-01-12
Instana				Unknown	link			cisagov	2022-01-12
Instructure				Unknown	link			cisagov	2022-01-12
Intel	Audio Development Kit			Unknown	link			cisagov	2021-12-16
Intel	Computer Vision Annotation Tool maintained by Intel			Unknown	link			cisagov	2021-12-16
Intel	Datacenter Manager			Unknown	link			cisagov	2021-12-16
Intel	Genomics Kernel Library			Unknown	link			cisagov	2021-12-16
Intel	oneAPI sample browser plugin for Eclipse			Unknown	link			cisagov	2021-12-16
Intel	Secure Device Onboard			Unknown	link			cisagov	2021-12-16
Intel	Sensor Solution Firmware Development Kit			Unknown	link			cisagov	2021-12-16
Intel	System Debugger			Unknown	link			cisagov	2021-12-16
Intel	System Studio			Unknown	link			cisagov	2021-12-16



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Internet Systems Consortium(ISC)	BIND 9			Not Affected	link	no JAVA Code		cisagov	2021-12-17
Internet Systems Consortium(ISC)	ISC DHCP, aka dhcpd			Not Affected	link	no JAVA Code		cisagov	2021-12-17
Internet Systems Consortium(ISC)	Kea DHCP			Not Affected	link	no JAVA Code		cisagov	2021-12-17
InterSystems				Unknown	link			cisagov	2022-01-12
Intland	codebeamer	<= 20.11-SP11, <= 21.09-SP3		Affected	link	A fix has been released for 20.11 and 21.09, but not yet for 21.04		cisagov	2022-01-12
IPro	Netgovern			Unknown				cisagov	2022-01-12
iRedMail				Unknown	link			cisagov	2022-01-12
Ironnet				Unknown	link			cisagov	2022-01-12
ISLONLINE				Unknown	link			cisagov	2022-01-12
Ivanti	Application Control for Linux			Not Affected	link			cisagov	2022-01-18
Ivanti	Application Control for Windows			Not Affected	link			cisagov	2022-01-18
Ivanti	Automation			Not Affected	link			cisagov	2022-01-18
Ivanti	Avalanche	6.2.2, 6.3.0 to 6.3.3		Affected	link			cisagov	2022-01-18
Ivanti	Avalanche Remote Control			Not Affected	link			cisagov	2022-01-18
Ivanti	CETerm (Naurtech)			Not Affected	link			cisagov	2022-01-18
Ivanti	Cherwell Asset Management (CAM)			Not Affected	link			cisagov	2022-01-18
Ivanti	Cherwell Service Management (CSM)			Not Affected	link			cisagov	2022-01-18
Ivanti	Connect Pro			Not Affected	link			cisagov	2022-01-18
Ivanti	ConnectPro (Termproxy)			Not Affected	link			cisagov	2022-01-18
Ivanti	Credential mgr (PivD Manager)			Not Affected	link			cisagov	2022-01-18
Ivanti	Discovery Classic			Not Affected	link			cisagov	2022-01-18
Ivanti	DSM			Not Affected	link			cisagov	2022-01-18
Ivanti	Environment Manager			Not Affected	link			cisagov	2022-01-18
Ivanti	GoldMine			Not Affected	link			cisagov	2022-01-18
Ivanti	HEAT Classic			Not Affected	link			cisagov	2022-01-18
Ivanti	IIRIS (Neurons for IIOT)			Not Affected	link			cisagov	2022-01-18
Ivanti	Incapptic Connect			Not Affected	link			cisagov	2022-01-18
Ivanti	Insight			Not Affected	link			cisagov	2022-01-18

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Ivanti	ITSM 6/7			Not Affected	link			cisagov	2022-01-18
Ivanti	Ivanti Asset Lifecycle Management			Not Affected	link			cisagov	2022-01-18
Ivanti	Ivanti Device Application Control			Not Affected	link			cisagov	2022-01-18
Ivanti	Ivanti Endpoint Manager			Not Affected	link			cisagov	2022-01-18
Ivanti	Ivanti Endpoint Security			Not Affected	link			cisagov	2022-01-18
Ivanti	Ivanti Environment Manager			Not Affected	link			cisagov	2022-01-18
Ivanti	Ivanti EPM - Cloud Service Appliance			Not Affected	link			cisagov	2022-01-18
Ivanti	Ivanti File Director	2019.1., 2020.1., 2020.3., 2021.1., 4.4.*	2021.3 HF2, 2021.1 HF1, 2020.3 HF2	Fixed	link			cisagov	2022-01-18
Ivanti	Ivanti Identity Director			Not Affected	link			cisagov	2022-01-18
Ivanti	Ivanti License Optimizer (ILO)			Not Affected	link			cisagov	2022-01-18
Ivanti	Ivanti Management Center			Not Affected	link			cisagov	2022-01-18
Ivanti	Ivanti Neurons Platform			Not Affected	link			cisagov	2022-01-18
Ivanti	Ivanti Performance Manager			Not Affected	link			cisagov	2022-01-18
Ivanti	Ivanti Security Controls (Patch ISec)			Not Affected	link	See More INFO for Ivanti Security Controls (Patch ISec) in the Advisory Page		cisagov	2022-01-18

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Ivanti	Ivanti Service Desk			Not Affected	link	Not Affected. Java is no longer required since version 2018.3U3 Customers on older versions can uninstall JRE on their ISD Servers for mitigation. This will disable indexing of Attachments and Documents for full-text search.		cisagov	2022-01-18
Ivanti	Ivanti Service Manager			Not Affected	link			cisagov	2022-01-18
Ivanti	Ivanti Service Manager for Neurons (Cloud)			Not Affected	link			cisagov	2022-01-18
Ivanti	Ivanti Voice			Not Affected	link			cisagov	2022-01-18
Ivanti	Ivanti Workspace Control			Not Affected	link			cisagov	2022-01-18
Ivanti	MI Appconnect			Not Affected	link			cisagov	2022-01-18
Ivanti	MI Email+			Not Affected	link			cisagov	2022-01-18
Ivanti	MI Go Client			Not Affected	link			cisagov	2022-01-18
Ivanti	MI MobileAtWork			Not Affected	link			cisagov	2022-01-18
Ivanti	MI Security Productivity Apps			Not Affected	link			cisagov	2022-01-18
Ivanti	Mi Tunnel App			Not Affected	link			cisagov	2022-01-18
Ivanti	MobileIron Access ZSO	All		Affected	link	Mitigated. No Impact		cisagov	2022-01-18
Ivanti	MobileIron BYOD Portal			Not Affected	link			cisagov	2022-01-18
Ivanti	MobileIron Cloud			Not Affected	link			cisagov	2022-01-18
Ivanti	MobileIron Cloud Connector			Not Affected	link			cisagov	2022-01-18
Ivanti	MobileIron Core	All		Affected	link	See Advisory details for mitigation instructions for MobileIron Core.		cisagov	2022-01-18

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Ivanti	MobileIron Core Connector	All		Affected	link	See Advisory details for mitigation instructions for Mobile-Iron Core Connector. See Advisory details for mitigation instructions for Mobile-Iron Sentry.		cisagov	2022-01-18
Ivanti	MobileIron Sentry (Core/Cloud)	9.13, 9.14		Affected	link			cisagov	2022-01-18
Ivanti	Patch MEM (Microsoft Endpoint Manager)			Not Affected	link			cisagov	2022-01-18
Ivanti	Patch OEM APIs			Not Affected	link			cisagov	2022-01-18
Ivanti	Performance Manager			Not Affected	link			cisagov	2022-01-18
Ivanti	Pulse Connect Secure			Not Affected	link			cisagov	2022-01-18
Ivanti	Pulse Desktop Client			Not Affected	link			cisagov	2022-01-18
Ivanti	Pulse Mobile Client			Not Affected	link			cisagov	2022-01-18
Ivanti	Pulse One			Not Affected	link			cisagov	2022-01-18
Ivanti	Pulse Policy Secure			Not Affected	link			cisagov	2022-01-18
Ivanti	Pulse Services Director			Not Affected	link			cisagov	2022-01-18
Ivanti	Pulse Virtual Traffic Manager			Not Affected	link			cisagov	2022-01-18
Ivanti	Pulse Web Application Firewall			Not Affected	link			cisagov	2022-01-18
Ivanti	Pulse ZTA			Not Affected	link			cisagov	2022-01-18
Ivanti	Risksense Threat and Vulnerability Management			Not Affected	link			cisagov	2022-01-18
Ivanti	SpeakEasy (add-on to Velocity)			Not Affected	link			cisagov	2022-01-18
Ivanti	SpeakEasy (WinCE)			Not Affected	link			cisagov	2022-01-18
Ivanti	Terminal Emulation and Industrial Browser Velocity			Not Affected	link			cisagov	2022-01-18
Ivanti	VelocityCE			Not Affected	link			cisagov	2022-01-18

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated	
Ivanti	Virtual Desktop Extender	10.31.0 – 10.34.0		Not Affected	link	Instructions to test your installations in announcement		cisagov	2022-01-18	
Ivanti	Wavelink License Server			Not Affected	link			cisagov	2022-01-18	
Ivanti	Xtraction			Not Affected	link			cisagov	2022-01-18	
Jamasoftware				Unknown	link			cisagov	2022-01-12	
Jamf	Jamf Pro			Affected	link			cisagov	2022-01-12	
Janitza	GridVis			Not Affected	link			cisagov	2022-01-05	
Jaspersoft				Unknown	link			cisagov	2022-01-12	
Jedox				Unknown	link			cisagov	2022-01-12	
Jenkins	CI/CD Core			Unknown				cisagov	2022-01-12	
Jenkins	Plugins			Unknown	link			cisagov	2021-12-16	
JetBrains	All .NET tools (ReSharper, Rider, ReSharper C++, dotTrace, dotMemory, dotCover, dotPeek)			Not Affected	link			cisagov	2022-01-12	
Jetbrains	Code With Me			Fixed	link			cisagov	2022-01-12	
JetBrains	Datalore			Not Affected	link			cisagov	2022-01-12	
JetBrains	Floating license server			30211	Fixed			link	cisagov	2022-01-12
JetBrains	Gateway			Not Affected	link			cisagov	2022-01-12	
JetBrains	Hub			2021.1.14080	Fixed			link	cisagov	2022-01-12
JetBrains	IntelliJ platform based IDEs (AppCode, CLion, DataGrip, DataSpell, GoLand, IntelliJ IDEA Ultimate/Community/Edu, PhpStorm, PyCharm Professional/Community/Edu, Rider, RubyMine, WebStorm)			Not Affected	link			cisagov	2022-01-12	
JetBrains	Kotlin			Not Affected	link			cisagov	2022-01-12	
JetBrains	Ktor			Not Affected	link			cisagov	2022-01-12	
JetBrains	MPS			Not Affected	link			cisagov	2022-01-12	
JetBrains	Space			Not Affected	link			cisagov	2022-01-12	
JetBrains	TeamCity			Not Affected	link			cisagov	2022-01-12	

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
JetBrains	ToolBox			Not Affected	link			cisagov	2022-01-12
JetBrains	UpSource		2020.1.1952	Fixed	link			cisagov	2022-01-12
JetBrains	YouTrack		Unknown	Fixed	link			cisagov	2022-01-12
	InCloud								
JetBrains	YouTrack Standalone		2021.4.35970	Fixed	link			cisagov	2022-01-12
JFROG				Unknown	link			cisagov	2022-01-12
Jitsi				Unknown	link			cisagov	2022-01-12
Jitterbit				Unknown	link			cisagov	2022-01-12
Johnson Controls	BCPro			Not Affected	link			cisagov	2021-12-21
Johnson Controls	CEM			Not Affected	link			cisagov	2021-12-21
Johnson Controls	AC2000 CEM			Not Affected	link			cisagov	2021-12-21
Johnson Controls	Hardware Products			Affected					
Johnson Controls	CloudVue Gateway			Not Affected	link			cisagov	2021-12-21
Johnson Controls	CloudVue Web			Not Affected	link			cisagov	2021-12-21
Johnson Controls	C • CURE-9000			Not Affected	link			cisagov	2021-12-21
Johnson Controls	C • CURE-9000			Not Affected	link			cisagov	2021-12-21
Johnson Controls	C • CURE-9000			Not Affected	link			cisagov	2021-12-21
Johnson Controls	C • CURE-9000			Not Affected	link			cisagov	2021-12-21
Johnson Controls	C • CURE-9000			Not Affected	link			cisagov	2021-12-21
Johnson Controls	DLS			Not Affected	link			cisagov	2021-12-21
Johnson Controls	Entrapass			Not Affected	link			cisagov	2021-12-21
Johnson Controls	exacqVision Client			Not Affected	link			cisagov	2021-12-21
Johnson Controls	exacqVision Server			Not Affected	link			cisagov	2021-12-21
Johnson Controls	exacqVision WebService			Not Affected	link			cisagov	2021-12-21
Johnson Controls	Facility Explorer			Not Affected	link			cisagov	2021-12-21
Johnson Controls	Illustra Cameras			Not Affected	link			cisagov	2021-12-21
Johnson Controls	Illustra Insight			Not Affected	link			cisagov	2021-12-21
Johnson Controls	iSTAR			Not Affected	link			cisagov	2021-12-21
Johnson Controls	Metasys Products and Tools			Not Affected	link			cisagov	2021-12-21
Johnson Controls	PowerSeries NEO			Not Affected	link			cisagov	2021-12-21
Johnson Controls	PowerSeries Pro			Not Affected	link			cisagov	2021-12-21
Johnson Controls	Qolsys IQ Panels			Not Affected	link			cisagov	2021-12-21
Johnson Controls	Sur-Gard Receivers			Not Affected	link			cisagov	2021-12-21
Johnson Controls	Tyco AI			Not Affected	link			cisagov	2021-12-21
Johnson Controls	victor			Not Affected	link			cisagov	2021-12-21
Johnson Controls	victor/ C • CURE-9000 Unified			Not Affected	link			cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Johnson Controls	victor/C • CURE-9000 Unified VideoEdge			Not Affected	link			cisagov	2021-12-21
Johnson Controls				Not Affected	link			cisagov	2021-12-21
Journyx				Unknown	link			cisagov	2022-01-12
jPOS	(ISO-8583) bridge			Not Affected	link			cisagov	2022-01-12
Jump Desktop				Unknown	link			cisagov	2022-01-12
Juniper Networks				Unknown	link			cisagov	2022-01-12
Justice Systems				Unknown	link			cisagov	2022-01-12
K15t				Unknown	link			cisagov	2022-01-12
K6				Unknown	link			cisagov	2022-01-12
Karakun				Unknown	link			cisagov	2022-01-12
Kaseya				Unknown	link			cisagov	2022-01-12
Keeper Security				Unknown	link			cisagov	2022-01-12
KEMP				Unknown	link			cisagov	2022-01-12
KEMP 2				Unknown	link			cisagov	2022-01-12
Kofax				Unknown	link			cisagov	2022-01-12
Konica				Unknown	link			cisagov	2022-01-12
Minolta									
Kronos				Unknown	link			cisagov	2022-01-12
UKG									
Kyberna				Unknown	link			cisagov	2022-01-12
L-Soft				Unknown	link			cisagov	2022-01-12
L3Harris				Unknown	link			cisagov	2022-01-12
Geospatial									
Lancom Systems				Unknown	link			cisagov	2022-01-12
Lansweeper				Unknown	link			cisagov	2022-01-12
Laserfiche				Unknown	link			cisagov	2022-01-12
LastPass				Unknown	link			cisagov	2022-01-12
LaunchDarkly				Unknown	link			cisagov	2022-01-12
Leanix				Unknown	link			cisagov	2022-01-12
Leica BIOSYSTEMS	Aperio AT2			Unknown	link			cisagov	2021-12-21
Leica BIOSYSTEMS	Aperio AT2			Unknown	link			cisagov	2021-12-21
Leica BIOSYSTEMS	Aperio CS2			Unknown	link			cisagov	2021-12-21
Leica BIOSYSTEMS	Aperio eSlide			Unknown	link			cisagov	2021-12-21
Leica BIOSYSTEMS	Aperio GT			Unknown	link			cisagov	2021-12-21
Leica BIOSYSTEMS	Aperio GT			Unknown	link			cisagov	2021-12-21
Leica BIOSYSTEMS	Aperio GT			Unknown	link			cisagov	2021-12-21
Leica BIOSYSTEMS	Aperio ImageScope			Unknown	link			cisagov	2021-12-21
Leica BIOSYSTEMS	Aperio ImageScope			Unknown	link			cisagov	2021-12-21
Leica BIOSYSTEMS	Aperio LV1			Unknown	link			cisagov	2021-12-21
Leica BIOSYSTEMS	Aperio SAM			Unknown	link			cisagov	2021-12-21
Leica BIOSYSTEMS	Aperio Scanner Administration Manager (SAM) Server for GT 450			Unknown	link			cisagov	2021-12-21

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Leica	Aperio			Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	VERSA		Unknown	link			cisagov	2021-12-21
Leica	Aperio			Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	WebViewer		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	DX		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	BOND		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	Controller		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	BOND RX		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	BOND RXm		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	BOND-		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	ADVANCE		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	BOND-III		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	BOND-MAX		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	CEREBRO		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	CytoVision		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	HistoCore		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	PEARL		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	HistoCore		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	PEGASUS		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	HistoCore		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	SPECTRA		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	CV		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	HistoCore		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	SPECTRA		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	ST		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	HistoCore		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	PIRIT ST		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	HistoCore		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	SPRING ST		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	Leica		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	ASP300S		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	Leica		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	SV5030		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	Leica ST4020		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	Leica ST5010		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	Leica ST5020		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	Leica TP1020		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	LIS Connect		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	PathDX		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	ThermoBrite		Unknown	link			cisagov	2021-12-21
Leica	BIOSYSTEMS	Elite		Unknown	link			cisagov	2021-12-21
Lenovo	BIOS/UEFI			Unknown	link			cisagov	2021-12-14
Lenovo	Chassis			Unknown	link			cisagov	2021-12-14
Lenovo	Management			Unknown	link			cisagov	2021-12-14
Lenovo	Module 2			Unknown	link			cisagov	2021-12-14
Lenovo	Commercial			Unknown	link			cisagov	2021-12-14
Lenovo	Vantage			Unknown	link			cisagov	2021-12-14
Lenovo	Confluent			Unknown	link			cisagov	2021-12-14
Lenovo	DSS-G			Unknown	link			cisagov	2021-12-14
Lenovo	Embedded			Unknown	link			cisagov	2021-12-14
Lenovo	System			Unknown	link			cisagov	2021-12-14
Lenovo	Management			Unknown	link			cisagov	2021-12-14
Lenovo	Java-based			Unknown	link			cisagov	2021-12-14
Lenovo	KVM clients			Unknown	link			cisagov	2021-12-14



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Lenovo	Fan Power Controller (FPC)			Unknown	link			cisagov	2021-12-14
Lenovo	Fan Power Controller2 (FPC2)			Unknown	link			cisagov	2021-12-14
Lenovo	Integrated Management Module II (IMM2)			Unknown	link			cisagov	2021-12-14
Lenovo	NetApp ONTAP Tools for VMware vSphere			Unknown	link	See NetApp advisory.		cisagov	2021-12-14
Lenovo	Network Switches running: Lenovo CNOS, Lenovo ENOS, IBM ENOS, or Brocade FOS			Unknown	link			cisagov	2021-12-14
Lenovo	Storage Management utilities			Unknown	link			cisagov	2021-12-14
Lenovo	System Management Module (SMM)			Unknown	link			cisagov	2021-12-14
Lenovo	System Management Module 2 (SMM2)			Unknown	link			cisagov	2021-12-14
Lenovo	System Update			Unknown	link			cisagov	2021-12-14
Lenovo	Thin Installer			Unknown	link			cisagov	2021-12-14
Lenovo	ThinkAgile HX			Unknown	link	Nutanix and VMware components only; hardware not affected. See Nutanix and VMWare advisories.		cisagov	2021-12-14
Lenovo	ThinkAgile VX			Unknown	link	VMware components only; hardware not affected. See VMWare advisory.		cisagov	2021-12-14
Lenovo	ThinkSystem 2x1x16 Digital KVM Switch - Type 1754D1T			Unknown	link			cisagov	2021-12-14

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Lenovo	ThinkSystem DE Series Storage			Unknown	link	See also NetApp advisory. See also NetApp advisory.		cisagov	2021-12-14
Lenovo	ThinkSystem DM Series Storage			Unknown	link			cisagov	2021-12-14
Lenovo	ThinkSystem DS Series Storage			Unknown	link			cisagov	2021-12-14
Lenovo	ThinkSystem Manager (TSM)			Unknown	link			cisagov	2021-12-14
Lenovo	Update Retriever			Unknown	link			cisagov	2021-12-14
Lenovo	Vantage			Unknown	link			cisagov	2021-12-14
Lenovo	XClarity Administrator (LXCA)			Unknown	link			cisagov	2021-12-14
Lenovo	XClarity Controller (XCC)			Unknown	link			cisagov	2021-12-14
Lenovo	XClarity Energy Manager (LXEM)			Unknown	link			cisagov	2021-12-14
Lenovo	XClarity Essentials (LXCE)			Unknown	link			cisagov	2021-12-14
Lenovo	XClarity Integrator (LXCI) for Microsoft Azure Log Analytics			Unknown	link			cisagov	2021-12-14
Lenovo	XClarity Integrator (LXCI) for Microsoft System Center			Unknown	link			cisagov	2021-12-14
Lenovo	XClarity Integrator (LXCI) for Nagios			Unknown	link			cisagov	2021-12-14
Lenovo	XClarity Integrator (LXCI) for ServiceNow			Unknown	link			cisagov	2021-12-14
Lenovo	XClarity Integrator (LXCI) for VMware vCenter			Unknown	link			cisagov	2021-12-14
Lenovo	XClarity Admin Center			Unknown	link			cisagov	2021-12-14
Lenovo	XClarity Mobile (LXCM)			Unknown	link			cisagov	2021-12-14
Lenovo	XClarity Orchestrator (LXCO)			Unknown	link			cisagov	2021-12-14

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Lenovo	XClarity Provisioning Manager (LXPM)			Unknown	link			cisagov	2021-12-14
LeoStream				Unknown	link			cisagov	2022-01-12
Let's Encrypt				Unknown	link			cisagov	2022-01-12
LibreNMS				Unknown	link			cisagov	2022-01-12
LifeRay				Unknown	link			cisagov	2022-01-12
LifeSize				Unknown	link			cisagov	2022-01-12
Lightbend				Unknown	link			cisagov	2022-01-12
Lime CRM				Unknown	link			cisagov	2022-01-12
LIONGARD				Unknown	link			cisagov	2022-01-12
LiquidFiles				Unknown	link			cisagov	2022-01-12
LiveAction				Unknown	link			cisagov	2022-01-12
Loftware				Unknown	link			cisagov	2022-01-12
LOGalyze	SIEM & log analyzer tool	v4.x		Affected	link	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)	cisagov	2021-12-17
LogiAnalytics				Unknown	link			cisagov	2022-01-12
LogicMonitor	LogicMonitor Platform			Unknown	link			cisagov	2022-01-12
LogMeIn				Unknown	link			cisagov	2022-01-12
LogRhythm				Unknown	link			cisagov	2022-01-12
Looker	Looker	21.0, 21.6, 21.12, 21.16, 21.18, 21.20		Affected	link			cisagov	2022-01-12
LucaNet				Unknown	link			cisagov	2022-01-12
Lucee				Unknown	link			cisagov	2022-01-12
Lyrasis	Fedora Repository			Not Affected	link	Fedora Repository is unaffiliated with Fedora Linux. Uses logback and explicitly excludes log4j.		cisagov	2021-12-14
MailStore				Unknown	link			cisagov	2022-01-12
Maltego				Unknown	link			cisagov	2022-01-12
ManageEngine				Unknown	link			cisagov	2022-01-12
Zoho ManageEngine	ADAudit Plus			Unknown	link			cisagov	2021-12-16
Zoho ManageEngine	ADManager Plus			Unknown	link			cisagov	2021-12-16
Zoho ManageEngine	Analytics Plus			Unknown	link			cisagov	2021-12-16
Zoho ManageEngine	Cloud			Unknown	link			cisagov	2021-12-16
Zoho ManageEngine	Security Plus			Unknown	link			cisagov	2021-12-16
Zoho ManageEngine	DataSecurity Plus			Unknown	link			cisagov	2021-12-16
Zoho ManageEngine	EventLog Analyzer			Unknown	link			cisagov	2021-12-16

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
ManageEngine	Exchange Reporter Plus			Unknown	link			cisagov	2021-12-16
ManageEngine	Log360			Unknown	link			cisagov	2021-12-16
ManageEngine	Log360 UEBA			Unknown	link			cisagov	2021-12-16
ManageEngine	M365 Manager Plus			Unknown	link			cisagov	2021-12-16
ManageEngine	M365 Security Plus			Unknown	link			cisagov	2021-12-16
ManageEngine	RecoveryManager Plus			Unknown	link			cisagov	2021-12-16
ManageEngine	AD SelfService Plus			Not Affected				cisagov	2021-12-27
ManageEngine	Servicedesk Plus	11305 and below		Affected	link			cisagov	2021-12-15
MariaDB	All			Unknown	link			cisagov	2022-01-12
MathWorks	MathWorks general release desktop or server products			Not Affected	link			cisagov	2022-01-18
MathWorks	MATLAB			Not Affected	link			cisagov	2022-01-18
Matillion	Matillion ETL		1.59.10+	Fixed	link			cisagov	2022-11-01
Matomo				Unknown	link			cisagov	2022-01-12
Mattermost				Unknown	link			cisagov	2022-01-12
FocalBoard									
McAfee	Data Exchange Layer (DXL) Client			Unknown				cisagov	2021-12-20
McAfee	Data Loss Prevention (DLP) Discover			Unknown				cisagov	2021-12-20
McAfee	Data Loss Prevention (DLP) Endpoint for Mac			Unknown				cisagov	2021-12-20
McAfee	Data Loss Prevention (DLP) Endpoint for Windows			Unknown				cisagov	2021-12-20
McAfee	Data Loss Prevention (DLP) Monitor			Unknown				cisagov	2021-12-20
McAfee	Data Loss Prevention (DLP) Prevent			Unknown				cisagov	2021-12-20
McAfee	Endpoint Security (ENS) for Linux			Unknown				cisagov	2021-12-20
McAfee	Endpoint Security (ENS) for Mac			Unknown				cisagov	2021-12-20

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
McAfee	Endpoint Security (ENS) for Windows			Unknown				cisagov	2021-12-20
McAfee	Enterprise Security Manager (ESM)		11.5.3	Fixed	link			cisagov	2021-12-20
McAfee	ePolicy Orchestrator Agent Handlers (ePO-AH)			Unknown				cisagov	2021-12-20
McAfee	ePolicy Orchestrator Application Server (ePO)		5.10 CU11	Fixed	link			cisagov	2021-12-20
McAfee	Host Intrusion Prevention (Host IPS)			Unknown				cisagov	2021-12-20
McAfee	Management of Native Encryption (MNE)			Unknown				cisagov	2021-12-20
McAfee	McAfee Active Response (MAR)			Unknown				cisagov	2021-12-20
McAfee	McAfee Agent (MA)			Unknown				cisagov	2021-12-20
McAfee	McAfee Application and Change Control (MACC) for Linux			Unknown				cisagov	2021-12-20
McAfee	McAfee Application and Change Control (MACC) for Windows			Unknown				cisagov	2021-12-20
McAfee	McAfee Client Proxy (MCP) for Mac			Unknown				cisagov	2021-12-20
McAfee	McAfee Client Proxy (MCP) for Windows			Unknown				cisagov	2021-12-20
McAfee	McAfee Drive Encryption (MDE)			Unknown				cisagov	2021-12-20
McAfee	McAfee Security for Microsoft Exchange (MSME)			Unknown				cisagov	2021-12-20
McAfee	McAfee Security for Microsoft Exchange (MSME)			Unknown				cisagov	2021-12-20

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
McAfee	McAfee Security for Microsoft SharePoint (MSMS)			Unknown				cisagov	2021-12-20
McAfee	Network Security Manager (NSM)			Unknown				cisagov	2021-12-20
McAfee	Network Security Platform (NSP)			Unknown				cisagov	2021-12-20
McAfee	Policy Auditor			Unknown				cisagov	2021-12-20
McAfee	Threat Intelligence Exchange (TIE)			Unknown	link	Latest status in linked Security Bulletin		cisagov	2021-12-20
McAfee	Web Gateway (MWG)			Unknown	link			cisagov	2021-12-20
Medtronic	MEINBERG			Unknown	link			cisagov	2021-12-21
MEINBERG	LANTIME and microSync			Unknown	link			cisagov	2022-01-12
Meltano	Meltano			Unknown	link	Project is written in Python		cisagov	2022-01-12
Memurai	Data			Unknown	link			cisagov	2022-01-12
Micro Focus	Protector		10.20, 10.30, 10.40, 10.50, 10.60, 10.70, 10.80, 10.90, 10.91, 11.00	Fixed	link		https://portal.microfocus.com/s/article/KM000003050	cisagov	2021-12-13
Microsoft	Azure API Gateway			Unknown	link			cisagov	2022-01-12
Microsoft	Azure Application Gateway			Unknown	link			cisagov	2022-01-12
Microsoft	Azure Data lake store java	< 2.3.10		Affected	link			cisagov	2022-01-12
Microsoft	Azure Data lake store java	< 2.3.10		Affected	link			cisagov	2022-01-12
Microsoft	Azure DevOps			Unknown	link			cisagov	2022-01-12
Microsoft	Azure DevOps Server	2019.0 - 2020.1		Affected	link			cisagov	2022-01-12
Microsoft	Azure Traffic Manager			Unknown	link			cisagov	2022-01-12
Microsoft	Team Foundation Server	2018.2+		Affected	link			cisagov	2022-01-12
Microstrategy				Unknown	link			cisagov	2022-01-12
Midori	Global			Unknown	link			cisagov	2022-01-12
Mikrotik				Unknown	link			cisagov	2022-01-12
Milestone sys				Unknown	link			cisagov	2022-01-12
Mimecast				Unknown	link			cisagov	2022-01-12
Minecraft				Unknown	link			cisagov	2022-01-12
Mirantis				Unknown	link			cisagov	2022-01-12
Miro				Unknown	link			cisagov	2022-01-12
Mitel				Unknown	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
MMM Group	Control software of all MMM series			Unknown	link			cisagov	2022-01-05
MMM Group	RUMED360 Cycles, RUMED360 Cycles View, RUMED360 Sicon, RUMED360 ISA-Server			Unknown	link			cisagov	2022-01-05
MongoDB	All other components of MongoDB Atlas (including Atlas Database, Data Lake, Charts)			Unknown	link			cisagov	2022-01-12
MongoDB	MongoDB Atlas Search			Unknown	link			cisagov	2022-01-12
MongoDB	MongoDB Community Edition (including Community Server, Cloud Manager, Community Kubernetes Operators)			Unknown	link			cisagov	2022-01-12
MongoDB	MongoDB Drivers			Unknown	link			cisagov	2022-01-12
MongoDB	MongoDB Enterprise Advanced (including Enterprise Server, Ops Manager, Enterprise Kubernetes Operators)			Unknown	link			cisagov	2022-01-12
MongoDB	MongoDB Realm (including Realm Database, Sync, Functions, APIs)			Unknown	link			cisagov	2022-01-12
MongoDB	MongoDB Tools (including Compass, Database Shell, VS Code Plugin, Atlas CLI, Database Connectors)			Unknown	link			cisagov	2022-01-12
Moodle				Unknown	link			cisagov	2022-01-12
MoogSoft				Unknown	link			cisagov	2022-01-12
Motorola Avigilon				Unknown	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Moxa				Not Affected	link	Moxa is investigating to determine if any of our products are affected by this vulnerability. At the time of publication, none of Moxa's products are affected.		cisagov	2022-01-19
Mulesoft				Unknown	link	This advisory is available to customers only and has not been reviewed by CISA.		cisagov	2022-01-12
Mulesoft	Anypoint Studio	7.x		Affected	link	This advisory is available to account holders only and has not been reviewed by CISA.		cisagov	2021-12-15
Mulesoft	Cloudhub			Unknown	link	This advisory is available to account holders only and has not been reviewed by CISA.		cisagov	2021-12-15
Mulesoft	Mule Agent	6.x		Affected	link	This advisory is available to account holders only and has not been reviewed by CISA.		cisagov	2021-12-15



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Mulesoft	Mule Runtime	3.x, 4.x		Affected	link	This advisory is available to account holders only and has not been reviewed by CISA.		cisagov	2021-12-15
N-able				Unknown	link			cisagov	2022-01-12
Nagios				Unknown	link			cisagov	2022-01-12
NAKIVO				Unknown	link			cisagov	2022-01-12
National Instruments	OptimalPlus	Vertica, Cloudera, Logstash		Affected	link	(Limited to deployments running Vertica, Cloudera, or Logstash) Contact Technical Support		cisagov	2022-01-05
Neo4j	Neo4j Graph Database	>4.2, <4..2.12		Affected				cisagov	2021-12-13
Netapp	Multiple NetApp products			Unknown	link			cisagov	2022-01-12
Netcup				Unknown	link			cisagov	2022-01-12
NetGate				Unknown	link			cisagov	2022-01-12
PFSense									
Netwrix				Unknown	link			cisagov	2022-01-12
New Relic	Containerized Private Minion (CPM)		3.0.57	Fixed	link	New Relic is in the process of revising guidance/documentation, however the fix version remains sufficient.	Security Bulletin NR21-04	cisagov	2021-12-18
New Relic	New Relic Java Agent	<7.4.3		Affected	link	Initially fixed in 7.4.2, but additional vulnerability found	New Relic tracking, covers CVE-2021-44228, CVE-2021-45046	cisagov	2021-12-20
NextCloud				Unknown	link			cisagov	2022-01-12
Nextflow	Nextflow			Not Affected	link			cisagov	2021-12-21
Nexus Group				Unknown	link			cisagov	2022-01-12
Nice Software (AWS) EnginFRAME				Unknown	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
NinjaRMM				Unknown	link	This advisory is available to customers only and has not been reviewed by CISA		cisagov	2022-01-12
Nomachine				Unknown	link			cisagov	2022-01-12
NoviFlow				Unknown	link			cisagov	2022-01-12
Nulab	Backlog		N/A (SaaS)	Fixed	link			cisagov	2022-01-12
Nulab	Backlog Enterprise (On-premises)		< 1.11.7	Fixed	link			cisagov	2022-01-12
Nulab	Cacao		N/A (SaaS)	Fixed	link			cisagov	2022-01-12
Nulab	Cacao Enterprise (On-premises)		< 4.0.4	Fixed	link			cisagov	2022-01-12
Nulab	Typetalk		N/A (SaaS)	Fixed	link			cisagov	2022-01-12
Nutanix	AHV			Not Affected	link			cisagov	2021-12-20
Nutanix	AOS			Not Affected	link			cisagov	2021-12-20
Nutanix	AOS		STS (including Prism Element)	Fixed	link	Patched in 6.0.2.4, available on the Portal for download.		cisagov	2021-12-20
Nutanix	Beam			Unknown	link	Saas-Based Product. See Advisory.		cisagov	2021-12-20
Nutanix	BeamGov			Unknown	link	Saas-Based Product. See Advisory.		cisagov	2021-12-20
Nutanix	Calm			Not Affected	link			cisagov	2021-12-20
Nutanix	Calm Tunnel VM			Not Affected	link			cisagov	2021-12-20
Nutanix	Collector			Not Affected	link			cisagov	2021-12-20
Nutanix	Collector Portal			Unknown	link	Saas-Based Product. See Advisory.		cisagov	2021-12-20
Nutanix	Data Lens			Unknown	link	Saas-Based Product. See Advisory.		cisagov	2021-12-20
Nutanix	Era			Not Affected	link			cisagov	2021-12-20

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Nutanix	File Analytics	2.1.x, 2.2.x, 3.0+		Affected	link	Mitigated in version 3.0.1 which is available on the Portal for download. Mitigation is available here		cisagov	2021-12-20
Nutanix	Files			Not Affected	link			cisagov	2021-12-20
Nutanix	Flow			Not Affected	link			cisagov	2021-12-20
Nutanix	Flow Security Cental			Unknown	link	Saas-Based Procu <sup>t</sup> . See Advisory.		cisagov	2021-12-20
Nutanix	Foundation			Not Affected	link			cisagov	2021-12-20
Nutanix	Frame			Unknown	link	Saas-Based Procu <sup>t</sup> . See Advisory.		cisagov	2021-12-20
Nutanix	FrameGov			Unknown	link	Saas-Based Procu <sup>t</sup> . See Advisory.		cisagov	2021-12-20
Nutanix	FSCVM			Not Affected	link			cisagov	2021-12-20
Nutanix	Insights			Unknown	link	Saas-Based Procu <sup>t</sup> . See Advisory.		cisagov	2021-12-20
Nutanix	Karbon	All		Affected	link	Mitigation is available here		cisagov	2021-12-20
Nutanix	Karbon Platform Service			Unknown	link	Saas-Based Procu <sup>t</sup> . See Advisory.		cisagov	2021-12-20
Nutanix	LCM			Not Affected	link			cisagov	2021-12-20
Nutanix	Leap			Unknown	link	Saas-Based Procu <sup>t</sup> . See Advisory.		cisagov	2021-12-20
Nutanix	Mine	All		Affected	link	Mitigation is available here		cisagov	2021-12-20
Nutanix	Move			Not Affected	link			cisagov	2021-12-20
Nutanix	MSP	All		Affected	link	Mitigation is available here		cisagov	2021-12-20
Nutanix	NCC			Not Affected	link			cisagov	2021-12-20
Nutanix	NGT			Not Affected	link			cisagov	2021-12-20

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Nutanix	Objects	All		Affected	link	Mitigation is available here		cisagov	2021-12-20
Nutanix	Prism Central		All	Fixed	link	Patched in 2021-9.0.3, available on the Portal for download.		cisagov	2021-12-20
Nutanix	Sizer			Unknown	link	SaaS-Based Product. See Advisory.		cisagov	2021-12-20
Nutanix	Volumes			Not Affected	link			cisagov	2021-12-20
Nutanix	Witness VM	All		Affected	link	Mitigation is available here		cisagov	2021-12-20
Nutanix	X-Ray			Not Affected	link			cisagov	2021-12-20
Nvidia				Unknown	link			cisagov	2022-01-12
NXLog				Unknown	link			cisagov	2022-01-12
Objectif Lune				Unknown	link			cisagov	2022-01-12
OCLC				Unknown	link			cisagov	2022-01-12
Octopus				Unknown	link			cisagov	2022-01-12
Okta	Advanced Server Access			Unknown	link			cisagov	2021-12-12
Okta	Okta Access Gateway			Unknown	link			cisagov	2021-12-12
Okta	Okta AD Agent			Unknown	link			cisagov	2021-12-12
Okta	Okta Browser Plugin			Unknown	link			cisagov	2021-12-12
Okta	Okta IWA Web Agent			Unknown	link			cisagov	2021-12-12
Okta	Okta LDAP Agent			Unknown	link			cisagov	2021-12-12
Okta	Okta Mobile			Unknown	link			cisagov	2021-12-12
Okta	Okta On-Prem MFA Agent	< 1.4.6		Affected	link			cisagov	2021-12-12
Okta	Okta RADIUS Server Agent	< 2.17.0		Affected	link			cisagov	2021-12-12
Okta	Okta Verify			Unknown	link			cisagov	2021-12-12
Okta	Okta Workflows			Unknown	link			cisagov	2021-12-12
Onespan				Unknown	link			cisagov	2022-01-12
Opengear				Unknown	link			cisagov	2022-01-12
OpenMRS				Unknown	link			cisagov	2022-01-12
TALK									
OpenNMS				Unknown	link			cisagov	2022-01-12
OpenSearch				Unknown	link			cisagov	2022-01-12
OpenText				Unknown	link			cisagov	2021-12-23
Opto 22	GROOV-ARI, GROOV-ARI-BASE, GROOV-ARI-SNAP	< 4.3g	4.3g	Fixed	link	The Log4j vulnerability affects all products running groov View software		cisagov	2022-01-13

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Opto 22	GROOV-AT1, GROOV-AT1-SNAP	< 4.3g	4.3g	Fixed	link	The Log4j vulnerability affects all products running groov View software		cisagov	2022-01-13
Opto 22	GROOV-SVR-WIN, GROOV-SVR-WIN-BASE, GROOV-SVR-WIN-SNAP	< 4.3g	4.3g	Fixed	link	The Log4j vulnerability affects all products running groov View software		cisagov	2022-01-13
Opto 22	GRV-EPIC-PR1, GRV-EPIC-PR2	< 3.3.2	3.3.2	Fixed	link	The Log4j vulnerability affects all products running groov View software		cisagov	2022-01-13
Oracle				Unknown	link	The support document is available to customers only and has not been reviewed by CISA		cisagov	2021-12-17
Oracle	Enterprise Manager	13.5, 13.4 & 13.3.2		Affected	link	Patch status and other security guidance is restricted to Oracle account/support members. The support document is available to customers only and has not been reviewed by CISA.		cisagov	2021-12-17

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Oracle	Exadata	<21.3.4		Affected	link	Patch status and other security guidance is restricted to Oracle ac-count/support members. The support document is available to customers only and has not been reviewed by CISA.		cisagov	2021-12-17
Orgavision				Unknown	link			cisagov	2022-01-12
Osirium	PAM			Unknown	link			cisagov	2022-01-12
Osirium	PEM			Unknown	link			cisagov	2022-01-12
Osirium	PPA			Unknown	link			cisagov	2022-01-12
OTRS				Unknown	link			cisagov	2022-01-12
OVHCloud				Unknown	link			cisagov	2022-01-12
OvnCloud				Unknown	link			cisagov	2022-01-12
OxygenXML	Author			Unknown		https://www.oxygenxml.com/security/advisory/CVE-2021-44228.html		cisagov	2021-12-17
OxygenXML	Developer			Unknown		https://www.oxygenxml.com/security/advisory/CVE-2021-44228.html		cisagov	2021-12-17
OxygenXML	Editor			Unknown		https://www.oxygenxml.com/security/advisory/CVE-2021-44228.html		cisagov	2021-12-17
OxygenXML	Oxygen Content Fusion	2.0, 3.0, 4.1		Affected		https://www.oxygenxml.com/security/advisory/CVE-2021-44228.html		cisagov	2021-12-17

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
OxygenXML	Oxygen Feedback Enterprise	1.4.4 & older		Affected		https://www.oxygenxml.com/security/advisory/CVE-2021-44228.html		cisagov	2021-12-17
OxygenXML	Oxygen License Server	v22.1 to v24.0		Affected		https://www.oxygenxml.com/security/advisory/CVE-2021-44228.html		cisagov	2021-12-17
OxygenXML	Oxygen PDF Chemistry	v22.1, 23.0, 23.1, 24.0		Affected		https://www.oxygenxml.com/security/advisory/CVE-2021-44228.html		cisagov	2021-12-17
OxygenXML	Oxygen SDK			Unknown		https://www.oxygenxml.com/security/advisory/CVE-2021-44228.html		cisagov	2021-12-17
OxygenXML	Plugins (see advisory link)			Unknown		https://www.oxygenxml.com/security/advisory/CVE-2021-44228.html		cisagov	2021-12-17
OxygenXML	Publishing Engine			Unknown		https://www.oxygenxml.com/security/advisory/CVE-2021-44228.html		cisagov	2021-12-17

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
OxygenXML	Web Author			Unknown		https://www.oxygenxml.com/security/advisory/CVE-2021-44228.html		cisagov	2021-12-17
OxygenXML	WebHelp			Unknown		https://www.oxygenxml.com/security/advisory/CVE-2021-44228.html		cisagov	2021-12-17
PagerDuty	PagerDuty SaaS			Unknown	link	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		cisagov	2021-12-21
QF-Test				Unknown	link			cisagov	2022-01-12
Qlik				Unknown	link			cisagov	2022-01-12
QMATIC	Appointment Booking	2.4+		Affected	link	Update to v. 2.8.2 which contains log4j 2.16 applied 2021-12-15		cisagov	2021-12-21
QMATIC	Appointment Booking	Cloud/Managed Service		Affected	link	log4j 2.16 applied 2021-12-15		cisagov	2021-12-21
QMATIC	Insights	Cloud		Affected	link	log4j 2.16 applied 2021-12-16		cisagov	2021-12-21
QMATIC	Orchestra Central			Not Affected	link			cisagov	2021-12-21



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated		
QNAP	Runecast Analyzer		6.0.3	Unknown	<a href="#">link</a>	This advisory is available to customers only and has not been reviewed by CISA “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.” “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.”		cisagov	2022-01-12		
QOPPA				Unknown	<a href="#">link</a>			cisagov	2022-01-12		
QSC				Unknown	<a href="#">link</a>			cisagov	2022-01-12		
Q-SYS				Unknown	<a href="#">link</a>			cisagov	2022-01-12		
QT					<a href="#">link</a>			cisagov	2022-01-12		
Quest				Unknown	<a href="#">link</a>			cisagov	2022-01-12		
Global											
Runecast				Fixed	<a href="#">link</a>			cisagov	2022-01-12		
SAE-IT											
SAFE				Unknown	<a href="#">link</a>			cisagov	2022-01-12		
FME	Unknown	<a href="#">link</a>					cisagov	2022-01-12			
Server											
SAGE											
SailPoint											
Salesforce	Analytics Cloud			Unknown	<a href="#">link</a>			cisagov	2021-12-15		
Salesforce	B2C Commerce Cloud			Unknown	<a href="#">link</a>			cisagov	2021-12-15		

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Salesforce	ClickSoftware (As-a-Service)			Unknown	link	“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.”		cisagov	2021-12-15
Salesforce	ClickSoftware (On-Premise)			Unknown	link	“Please contact Customer Support.”		cisagov	2021-12-15
Salesforce	Community Cloud			Unknown	link	“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.”		cisagov	2021-12-15
Salesforce	Data.com			Unknown	link	“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.”		cisagov	2021-12-15
Salesforce	DataLoader		<=53.0.0	Fixed	link			cisagov	2021-12-22

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Salesforce	Datorama			Unknown	link	“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.”		cisagov	2021-12-15
Salesforce	Evergage (Interaction Studio)			Unknown	link	“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.”		cisagov	2021-12-15
Salesforce	Force.com			Unknown	link	“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.”		cisagov	2021-12-15

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Salesforce	Heroku			Unknown	link	“Heroku is reported to not be affected by CVE-2021-44228; no further action is necessary at this time.”		cisagov	2021-12-15
Salesforce	Marketing Cloud			Unknown	link	“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.”		cisagov	2021-12-15
Salesforce	MuleSoft (Cloud)			Unknown	link	“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.”		cisagov	2021-12-15
Salesforce	MuleSoft (On-Premise)			Unknown	link	“Please contact Customer Support.”		cisagov	2021-12-15
Salesforce	Pardot			Unknown	link	“Pardot is reported to be affected by CVE-2021-44228. The service is being updated to remediate the vulnerability identified in CVE-2021-44228.”		cisagov	2021-12-15

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Salesforce	Sales Cloud			Unknown	link	“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.”		cisagov	2021-12-15
Salesforce	Service Cloud			Unknown	link	“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.”		cisagov	2021-12-15
Salesforce	Slack			Unknown	link	“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.”		cisagov	2021-12-15

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Salesforce	Social Studio			Unknown	link	“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.”		cisagov	2021-12-15
Salesforce	Tableau (On-Premise)		< 2021.4.1	Fixed	link	Fixed in 2021.4.1		cisagov	2021-12-16
Salesforce	Tableau (Online)			Unknown	link	“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.”		cisagov	2021-12-15
Samsung Electronics America	Knox Admin Portal			Not Affected	link			cisagov	2022-01-17
Samsung Electronics America	Knox Asset Intelligence			Not Affected	link			cisagov	2022-01-17
Samsung Electronics America	Knox Configure			Not Affected	link			cisagov	2022-01-17
Samsung Electronics America	Knox E-FOTA One			Not Affected	link			cisagov	2022-01-17
Samsung Electronics America	Knox Guard			Not Affected	link			cisagov	2022-01-17
Samsung Electronics America	Knox License Management			Not Affected	link			cisagov	2022-01-17

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Samsung Electronics America	Knox Manage		Cloud	Fixed	link			cisagov	2022-01-17
Samsung Electronics America	Knox Managed Services Provider (MSP)			Not Affected	link			cisagov	2022-01-17
Samsung Electronics America	Knox Mobile Enrollment			Not Affected	link			cisagov	2022-01-17
Samsung Electronics America	Knox Reseller Portal		Cloud	Fixed	link			cisagov	2022-01-17
Sangoma SAP				Unknown Unknown	link link	This advisory is available to customers only and has not been reviewed by CISA		cisagov cisagov	2022-01-12 2021-12-17
SAP Advanced Platform				Unknown	link	This advisory is available to customers only and has not been reviewed by CISA		cisagov	2021-12-17
SAP BusinessObjects				Unknown	link	The support document is available to customers only and has not been reviewed by CISA		cisagov	2021-12-17
SAS SASSAFRAS				Unknown	link			cisagov	2022-01-12
Savignano software solutions				Unknown	link			cisagov	2022-01-12
SBT	SBT	<1.5.6		Affected	link			cisagov	2021-12-15
ScaleComputing				Unknown	link	This advisory is available to customers only and has not been reviewed by CISA		cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
ScaleFusion				Unknown	link			cisagov	2022-01-12
Mobile-Lock Pro									
Schneider Electric	EASYFIT	Current software and earlier		Affected	link			cisagov	2021-12-20
Schneider Electric	Ecoreal XL	Current software and earlier		Affected	link			cisagov	2021-12-20
Schneider Electric	EcoStruxure IT Expert		Cloud	Fixed				cisagov	2021-12-20
Schneider Electric	EcoStruxure IT Gateway		V1.5.0 to V1.13.0	Fixed	link			cisagov	2021-12-20
Schneider Electric	Eurotherm Data Reviewer	V3.0.2 and prior		Affected	link			cisagov	2021-12-20
Schneider Electric	Facility Expert Small Business		Cloud	Fixed	link			cisagov	2021-12-20
Schneider Electric	MSE	Current software and earlier		Affected	link			cisagov	2021-12-20
Schneider Electric	NetBotz750/755	Software versions 5.0 through 5.3.0		Affected	link			cisagov	2021-12-20
Schneider Electric	NEW630	Current software and earlier		Affected	link			cisagov	2021-12-20
Schneider Electric	SDK BOM	Current software and earlier		Affected	link			cisagov	2021-12-20
Schneider Electric	SDK-Docgen	Current software and earlier		Affected	link			cisagov	2021-12-20
Schneider Electric	SDK-TNC	Current software and earlier		Affected	link			cisagov	2021-12-20
Schneider Electric	SDK-UMS	Current software and earlier		Affected	link			cisagov	2021-12-20
Schneider Electric	SDK3D2DRenderer	Current software and earlier		Affected	link			cisagov	2021-12-20
Schneider Electric	SDK3D360Widget	Current software and earlier		Affected	link			cisagov	2021-12-20
Schneider Electric	Select and Config DATA	Current software and earlier		Affected	link			cisagov	2021-12-20
Schneider Electric	SNC-API	Current software and earlier		Affected	link			cisagov	2021-12-20
Schneider Electric	SNC-CMM	Current software and earlier		Affected	link			cisagov	2021-12-20
Schneider Electric	SNCSEMTECH	Current software and earlier		Affected	link			cisagov	2021-12-20
Schneider Electric	SPIMV3	Current software and earlier		Affected	link			cisagov	2021-12-20
Schneider Electric	SWBEditor	Current software and earlier		Affected	link			cisagov	2021-12-20
Schneider Electric	SWBEngine	Current software and earlier		Affected	link			cisagov	2021-12-20
Schneider Electric	Wiser by SE platform		Cloud	Fixed				cisagov	2021-12-20
Schweitzer Engineering Laboratories				Unknown	link			cisagov	2021-12-21
SCM Manager				Unknown	link			cisagov	2022-01-12
ScreenBeam				Unknown	link			cisagov	2022-01-12
SDL worldServer				Unknown	link			cisagov	2022-01-12
Seagull Scientific				Unknown	link			cisagov	2022-01-12
SecurePoint Security				Unknown	link			cisagov	2022-01-12
Onion				Unknown	link			cisagov	2022-01-12



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Securonix	Extended Detection and Response (XDR)	All		Affected	link	Patching ongoing as of 12/10/2021		cisagov	2021-12-10
Securonix	Next Gen SIEM	All		Affected	link	Patching ongoing as of 12/10/2021		cisagov	2021-12-10
Securonix	Security Analytics and Operations Platform (SOAR)	All		Affected	link	Patching ongoing as of 12/10/2021		cisagov	2021-12-10
Securonix	SNYPR Application			Unknown	link			cisagov	2021-12-10
Securonix	User and Entity Behavior Analytics(UEBA)	All		Affected	link	Patching ongoing as of 12/10/2021		cisagov	2021-12-10
Seeburger				Unknown	link	This advisory is available to customers only and has not been reviewed by CISA.		cisagov	2022-01-12
SentinelOne				Unknown	link			cisagov	2022-01-12
Sentry				Unknown	link			cisagov	2022-01-12
SEP				Unknown	link			cisagov	2022-01-12
Server Eye				Unknown	link			cisagov	2022-01-12
ServiceNow				Unknown	link			cisagov	2022-01-12
Shibboleth				Unknown	link			cisagov	2022-01-12
Shibboleth	All Products			Not Affected	link			cisagov	2021-12-10
Shopify				Unknown	link			cisagov	2022-01-12
Siebel				Unknown	link			cisagov	2022-01-12
Siemens Energy	Affected Products			Unknown	link	Siemens requests: See pdf for the complete list of affected products, CSAF for automated parsing of data		cisagov	2021-12-21
Siemens Energy	Affected Products			Unknown	link	Siemens requests: See pdf for the complete list of affected products, CSAF for automated parsing of data		cisagov	2021-12-20

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Siemens Energy	Affected Products			Unknown	link	Siemens requests: See pdf for the complete list of affected products, CSAF for automated parsing of data		cisagov	2021-12-16
Siemens Healthineers	ATELLICA DATA MANAGER v1.1.1 / v1.2.1 / v1.3.1			Unknown	link	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.		cisagov	2021-12-22

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Siemens Healthineers	CENTRALINK	v16.0.2 / v16.0.3		Unknown	link	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.		cisagov	2021-12-22
Siemens Healthineers	Cios Flow S1 / Alpha / Spin VA30			Unknown	link	evaluation ongoing		cisagov	2021-12-22
Siemens Healthineers	Cios Select FD/I.I. VA21 / VA21-S3P			Unknown	link	evaluation ongoing		cisagov	2021-12-22
Siemens Healthineers	DICOM Proxy VB10A			Unknown	link	Workaround: remove the vulnerable class from the .jar file		cisagov	2021-12-22
Siemens Healthineers	go.All, Som10 VA20 / VA30 / VA40			Unknown	link	Workaround: In the meantime, we recommend preventing access to port 8090 from other devices by configuration of the hospital network.		cisagov	2021-12-22
Siemens Healthineers	go.Fit, Som10 VA30			Unknown	link	Workaround: In the meantime, we recommend preventing access to port 8090 from other devices by configuration of the hospital network.		cisagov	2021-12-22

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Siemens Healthineers	go.Now, Som10 VA10 / VA20 / VA30 / VA40			Unknown	link	Workaround: In the meantime, we recommend preventing access to port 8090 from other devices by configuration of the hospital network.		cisagov	2021-12-22
Siemens Healthineers	go.Open Pro, Som10 VA30 / VA40			Unknown	link	Workaround: In the meantime, we recommend preventing access to port 8090 from other devices by configuration of the hospital network.		cisagov	2021-12-22
Siemens Healthineers	go.Sim, Som10 VA30 / VA40			Unknown	link	Workaround: In the meantime, we recommend preventing access to port 8090 from other devices by configuration of the hospital network.		cisagov	2021-12-22
Siemens Healthineers	go.Top, Som10 VA20 / VA20A_SP5 / VA30 / VA40			Unknown	link	Workaround: In the meantime, we recommend preventing access to port 8090 from other devices by configuration of the hospital network.		cisagov	2021-12-22

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Siemens Healthineers	go.Up, Som10 VA10 / VA20 / VA30 / VA40			Unknown	link	Workaround: In the meantime, we recommend preventing access to port 8090 from other devices by configuration of the hospital network.		cisagov	2021-12-22
Siemens Healthineers	MAGNETOM AERA 1,5T, MAGNETOM PRISMA, MAGNETOM PRISMA FIT, MAGNETOM SKYRA 3T NU-MARIS/X VA30A			Unknown	link	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.		cisagov	2021-12-22
Siemens Healthineers	MAGNETOM Altea NU-MARIS/X VA20A			Unknown	link	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.		cisagov	2021-12-22

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Siemens Healthineers	MAGNETOM ALTEA, MAGNE-TOM LUMINA, MAGNE-TOM SOLA, MAGNE-TOM VIDA NU-MARIS/X VA31A			Unknown	<a href="#">link</a>	LOG4J is used in the context of the help system. Workaround: close port 8090 for standalone systems. Setup IP whitelist-ing for “need to access” systems to network port 8090 in case a second console is connected.		cisagov	2021-12-22
	MAGNETOM Amira NU-MARIS/X VA12M			Unknown	<a href="#">link</a>	LOG4J is used in the context of the help system. Workaround: close port 8090 for standalone systems. Setup IP whitelist-ing for “need to access” systems to network port 8090 in case a second console is connected.		cisagov	2021-12-22
	MAGNETOM Free.Max NU-MARIS/X VA40			Unknown	<a href="#">link</a>	LOG4J is used in the context of the help system. Workaround: close port 8090 for standalone systems. Setup IP whitelist-ing for “need to access” systems to network port 8090 in case a second console is connected.		cisagov	2021-12-22

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Siemens Healthineers	MAGNETOM Lumina NU-MARIS/X VA20A			Unknown	<a href="#">link</a>	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.		cisagov	2021-12-22
Siemens Healthineers	MAGNETOM Semptra NU-MARIS/X VA12M			Unknown	<a href="#">link</a>	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.		cisagov	2021-12-22
Siemens Healthineers	MAGNETOM Sola fit NU-MARIS/X VA20A			Unknown	<a href="#">link</a>	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.		cisagov	2021-12-22

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Siemens Healthineers	MAGNETOM Sola NU-MARIS/X VA20A			Unknown	link	LOG4J is used in the context of the help system. Workaround: close port 8090 for standalone systems. Setup IP whitelist-ing for “need to access” systems to network port 8090 in case a second console is connected.		cisagov	2021-12-22
				Unknown	link	LOG4J is used in the context of the help system. Workaround: close port 8090 for standalone systems. Setup IP whitelist-ing for “need to access” systems to network port 8090 in case a second console is connected.		cisagov	2021-12-22
				Unknown	link	LOG4J is used in the context of the help system. Workaround: close port 8090 for standalone systems. Setup IP whitelist-ing for “need to access” systems to network port 8090 in case a second console is connected.		cisagov	2021-12-22



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Siemens Healthineers	SENSIS DMCC / DMCM / TS / VM / PPWS / DS VD12A			Unknown	link	evaluation ongoing		cisagov	2021-12-22
Siemens Healthineers	Somatom Emotion Som5 VC50			Unknown	link	evaluation ongoing		cisagov	2021-12-22
Siemens Healthineers	Somatom Scope Som5 VC50			Unknown	link	evaluation ongoing		cisagov	2021-12-22
Siemens Healthineers	Syngo Carbon Space VA10A / VA10A-CUT2 / VA20A			Unknown	link	Workaround: remove the vulnerable class from the .jar file		cisagov	2021-12-22
Siemens Healthineers	Syngo MobileViewer VA10A			Unknown	link	The vulnerability will be patch/mitigated in upcoming releases/patches.		cisagov	2021-12-22
Siemens Healthineers	syngo Plaza VB20A / VB20A_HF01 - HF07 / VB30A / VB30A_HF01 / VB30A_HF02 / VB30B / VB30C / VB30C_HF01 - HF06 / VB30C_HF91			Unknown	link	Workaround: remove the vulnerable class from the .jar file		cisagov	2021-12-22
Siemens Healthineers	syngo Workflow MLR VB37A / VB37A_HF01 / VB37A_HF02 / VB37B / VB37B_HF01 - HF07 / VB37B_HF93 / VB37B_HF94 / VB37B_HF96			Unknown	link	Please contact your Customer Service to get support on mitigating the vulnerability.		cisagov	2021-12-22

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	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			Unknown	link	Workaround: remove the vulnerable class from the .jar file		cisagov	2021-12-22
Siemens Healthineers	syngo.via WebViewer VA13B / VA20A / VA20B			Unknown	link	Workaround: remove the vulnerable class from the .jar file		cisagov	2021-12-22
Siemens Healthineers	X.Ceed Somaris 10 VA40*			Unknown	link	Workaround: In the meantime, we recom- mend preventing access to port 8090 from other devices by configura- tion of the hospital network.		cisagov	2021-12-22
Siemens Healthineers	X.Cite Somaris 10 VA30/VA40			Unknown	link	Workaround: In the meantime, we recom- mend preventing access to port 8090 from other devices by configura- tion of the hospital network.		cisagov	2021-12-22

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Siemens	Affected Products			Unknown	link	Siemens requests: See pdf for the complete list of affected products, CSAF for automated parsing of data		cisagov	2021-12-22
Siemens	Affected Products			Unknown	link	Siemens requests: See pdf for the complete list of affected products, CSAF for automated parsing of data		cisagov	2021-12-19
Sierra Wireless	AirVantage and Octave cloud platforms			Unknown	link	These systems do not operate with the specific non-standard configuration required for CVE-2021-25046 and hence were not vulnerable to it.		cisagov	2022-01-12
Sierra Wireless				Unknown	link			cisagov	2022-01-05
Sierra Wireless Signald	AM/AMM servers			Unknown	link			cisagov	2022-01-05
				Unknown	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Silver Peak	Orchestrator, Silver Peak GMS			Unknown	link	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.		cisagov	2021-12-14
	SingleWire			Unknown	link	This advisory is available to customers only and has not been reviewed by CISA		cisagov	2022-01-12
	SISCO			Unknown	link			cisagov	2022-01-05
	Sitecore			Unknown	link			cisagov	2022-01-12
	Skillable			Unknown	link			cisagov	2022-01-12
	SLF4J			Unknown	link			cisagov	2022-01-12
	Slurm	Slurm		Not Affected	link			cisagov	2021-12-21
	SMA Solar Technology AG			Unknown	link			cisagov	2022-01-05
	SmartBear			Unknown	link			cisagov	2022-01-12
	SmileCDR			Unknown	link			cisagov	2022-01-12
	Sn0m			Unknown	link			cisagov	2022-01-12
	Snakemake	Snakemake		Not Affected	link			cisagov	2021-12-21
	Snow Software	Snow Commander	8.1 to 8.10.2	Fixed	link			cisagov	2022-01-12
	Snow Software	VM Access Proxy	v3.1 to v3.6	Fixed	link			cisagov	2022-01-12
	Snowflake			Unknown	link			cisagov	2022-01-12
	Snyk	Cloud Platform		Unknown	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Software AG				Unknown	<a href="#">link</a>			cisagov	2022-01-12
SolarWinds	Database Performance Analyzer (DPA)	2021.1.x, 2021.3.x, 2022.1.x		Affected	<a href="#">link</a>	For more information, please see the following KB article: <a href="#">link</a>		cisagov	2021-12-23
SolarWinds	Orion Platform			Unknown	<a href="#">link</a>			cisagov	2021-12-23
SolarWinds	Server & Application Monitor (SAM)	SAM 2020.2.6 and later		Affected	<a href="#">link</a>	For more information, please see the following KB article for the latest details specific to the SAM hotfix: <a href="#">link</a>		cisagov	2021-12-23
SonarSource				Unknown	<a href="#">link</a>			cisagov	2022-01-12
Sonatype	All Products			Not Affected	<a href="#">link</a>	Sonatype uses logback as the default logging solution as opposed to log4j. This means our software including Nexus Lifecycle, Nexus Firewall, Nexus Repository OSS and Nexus Repository Pro in versions 2.x and 3.x are NOT affected by the reported log4j vulnerabilities. We still advise keeping your software upgraded at the latest version.		cisagov	2021-12-29

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
SonicWall	Access Points			Unknown	link	Log4j2 not used in the SonicWall Access Points		cisagov	2021-12-12
SonicWall	Analytics			Unknown	link	Under Review		cisagov	2021-12-12
SonicWall	Analyzer			Unknown	link	Under Review		cisagov	2021-12-12
SonicWall	Capture Client & Capture Client Portal			Unknown	link	Log4j2 not used in the Capture Client.		cisagov	2021-12-12
SonicWall	Capture Security Appliance			Unknown	link	Log4j2 not used in the Capture Security appliance.		cisagov	2021-12-12
SonicWall	CAS			Unknown	link	Under Review		cisagov	2021-12-12
SonicWall	Email Security			Unknown	link	ES 10.0.11 and earlier versions are impacted		cisagov	2021-12-17
SonicWall	Gen5 Firewalls (EOS)			Unknown	link	Log4j2 not used in the appliance.		cisagov	2021-12-12
SonicWall	Gen6 Firewalls			Unknown	link	Log4j2 not used in the appliance.		cisagov	2021-12-12
SonicWall	Gen7 Firewalls			Unknown	link	Log4j2 not used in the appliance.		cisagov	2021-12-12
SonicWall	GMS			Unknown	link	Under Review		cisagov	2021-12-12
SonicWall	MSW			Unknown	link	Mysonicwall service doesn't use Log4j		cisagov	2021-12-12
SonicWall	NSM			Unknown	link	NSM On-Prem and SaaS doesn't use a vulnerable version		cisagov	2021-12-12
SonicWall	SMA 100			Unknown	link	Log4j2 not used in the SMA100 appliance.		cisagov	2021-12-12
SonicWall	SMA 1000			Unknown	link	Version 12.1.0 and 12.4.1 doesn't use a vulnerable version		cisagov	2021-12-12
SonicWall	SonicCore			Unknown	link	SonicCore doesn't use a Log4j2		cisagov	2021-12-12
SonicWall	SonicWall Switch			Unknown	link	Log4j2 not used in the SonicWall Switch.		cisagov	2021-12-12
SonicWall	WAF			Unknown	link	Under Review		cisagov	2021-12-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
SonicWall	WNM			Unknown	link	Log4j2 not used in the WNM.		cisagov	2021-12-12
SonicWall	WXA			Unknown	link	WXA doesn't use a vulnerable version		cisagov	2021-12-12
Sophos	Cloud Optix			Unknown	link	Users may have noticed a brief outage around 12:30 GMT as updates were deployed. There was no evidence that the vulnerabil-ity was exploited and to our knowledge no customers are impacted.		cisagov	2021-12-12
Sophos	Reflexion			Unknown	link	Reflexion does not run an ex-ploitable configuration.		cisagov	2021-12-12
Sophos	SG UTM (all versions)			Unknown	link	Sophos SG UTM does not use Log4j.		cisagov	2021-12-12
Sophos	SG UTM Manager (SUM) (all versions)			Not Affected	link	SUM does not use Log4j.		cisagov	2021-12-12
Sophos	Sophos Central			Unknown	link	Sophos Central does not run an ex-ploitable configuration.		cisagov	2021-12-12
Sophos	Sophos Firewall (all versions)			Unknown	link	Sophos Firewall does not use Log4j.		cisagov	2021-12-12
Sophos	Sophos Home			Unknown	link	Sophos Home does not use Log4j.		cisagov	2021-12-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Sophos	Sophos Mobile			Unknown	link	Sophos Mobile (in Central, SaaS, and on-premises) does not run an exploitable configuration.		cisagov	2021-12-12
Sophos	Sophos Mobile EAS Proxy	< 9.7.2		Affected	link	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. Power-Shell mode is not affected. Customers can download the Standalone EAS Proxy Installer version 9.7.2 from the Sophos website.		cisagov	2021-12-12
Sophos	Sophos ZTNA			Unknown	link	Sophos ZTNA does not use Log4j.		cisagov	2021-12-12
SOS Berlin				Unknown	link			cisagov	2022-01-12
Spacelabs Healthcare	ABP			Not Affected	link			cisagov	2022-01-05
Spacelabs Healthcare	CardioExpress			Not Affected	link			cisagov	2022-01-05
Spacelabs Healthcare	DM3 and DM4 Monitors			Unknown	link			cisagov	2022-01-05
Spacelabs Healthcare	Eclipse Pro			Unknown	link			cisagov	2022-01-05



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Spacelabs Healthcare	EVO			Unknown	link			cisagov	2022-01-05
Spacelabs Healthcare	Intesys Clinical Suite (ICS)			Unknown	link			cisagov	2022-01-05
Spacelabs Healthcare	Intesys Clinical Suite (ICS) Clinical Access Workstations			Unknown	link			cisagov	2022-01-05
Spacelabs Healthcare	Lifescreeen Pro			Unknown	link			cisagov	2022-01-05
Spacelabs Healthcare	Pathfinder			Unknown	link			cisagov	2022-01-05
Spacelabs Healthcare	SL			Not Affected	link			cisagov	2022-01-05
Spacelabs Healthcare	Qube			Not Affected	link			cisagov	2022-01-05
Spacelabs Healthcare	Qube Mini			Not Affected	link			cisagov	2022-01-05
Spacelabs Healthcare	SafeNSound		4.3.1	Fixed	link	Version >4.3.1 - Not Affected		cisagov	2022-01-05
Spacelabs Healthcare	Sentinel			Unknown	link			cisagov	2022-01-05
Spacelabs Healthcare	Spacelabs Cloud			Unknown	link			cisagov	2022-01-05
Spacelabs Healthcare	Ultraview SL			Not Affected	link			cisagov	2022-01-05
Spacelabs Healthcare	Xhibit Telemetry Receiver (XTR)			Not Affected	link			cisagov	2022-01-05
Spacelabs Healthcare	Xhibit, XC4			Not Affected	link			cisagov	2022-01-05
Spacelabs Healthcare	XprezzNet			Not Affected	link			cisagov	2022-01-05
Spacelabs Healthcare	Xprezzon			Not Affected	link			cisagov	2022-01-05
Spambrella Spigot				Unknown	link			cisagov	2022-01-12
Splunk	Data Stream Processor	DSP 1.0.x, DSP 1.1.x, DSP 1.2.x		Unknown	link			cisagov	2022-01-12
Splunk	IT Essentials Work App ID 5403	4.11, 4.10.x (Cloud only), 4.9.x		Affected	link			cisagov	2021-12-30
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	link			cisagov	2021-12-30
Splunk	Splunk Add-On for Java Management Extensions App ID 2647	5.2.0 and older		Affected	link			cisagov	2021-12-30
Splunk	Splunk Add-On for Tomcat App ID 2911	3.0.0 and older		Affected	link			cisagov	2021-12-30
Splunk	Splunk Application Performance Monitoring	Current		Affected	link			cisagov	2021-12-30
Splunk	Splunk Connect for Kafka	All versions prior to 2.0.4		Affected	link			cisagov	2021-12-30

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
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	link			cisagov	2021-12-30
Splunk	Splunk Enterprise Amazon Machine Image (AMI)	See Splunk Enterprise		Affected	link			cisagov	2021-12-30
Splunk	Splunk Enterprise Docker Container	See Splunk Enterprise		Affected	link			cisagov	2021-12-30
Splunk	Splunk Infrastructure Monitoring	Current		Affected	link			cisagov	2021-12-30
Splunk	Splunk Log Observer	Current		Affected	link			cisagov	2021-12-30
Splunk	Splunk Logging Library for Java	1.11.0 and older		Affected	link			cisagov	2021-12-30
Splunk	Splunk On-call / VictorOps	Current		Affected	link			cisagov	2021-12-30
Splunk	Splunk OVA for VMWare App ID 3216	4.0.3 and older		Affected	link			cisagov	2021-12-30
Splunk	Splunk OVA for VMWare Metrics App ID 5096	4.2.1 and older		Affected	link			cisagov	2021-12-30
Splunk	Splunk Real User Monitoring	Current		Affected	link			cisagov	2021-12-30
Splunk	Splunk Add-On for JBoss App ID 2954	3.0.0 and older		Affected	link			cisagov	2021-12-30
Splunk	Splunk Synthetics	Current		Affected	link			cisagov	2021-12-30
Splunk	Splunk UBA OVA	5.0.3a, 5.0.0		Affected	link			cisagov	2021-12-30
Splunk	Software Splunk VMWare OVA for ITSI App ID 4760	1.1.1 and older		Affected	link			cisagov	2021-12-30
Sprecher Automation Spring Boot				Unknown	link			cisagov	2022-01-12
				Unknown	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Spring	Spring Boot			Unknown	<a href="#">link</a>	Spring Boot users are only affected by this vulnerability if they have switched the default logging system to Log4J2		cisagov	2022-01-12
StarDog				Unknown	<a href="#">link</a>			cisagov	2022-01-12
STERIS	Advantage			Unknown	<a href="#">link</a>			cisagov	2021-12-22
STERIS	Advantage Plus			Unknown	<a href="#">link</a>			cisagov	2021-12-22
STERIS	AMSCO 2000 SERIES WASHER DISINFECTORS			Unknown	<a href="#">link</a>			cisagov	2021-12-22
STERIS	AMSCO 3000 SERIES WASHER DISINFECTORS			Unknown	<a href="#">link</a>			cisagov	2021-12-22
STERIS	AMSCO 400 MEDIUM STEAM STERILIZER			Unknown	<a href="#">link</a>			cisagov	2021-12-22
STERIS	AMSCO 400 SMALL STEAM STERILIZERS			Unknown	<a href="#">link</a>			cisagov	2021-12-22
STERIS	AMSCO 5000 SERIES WASHER DISINFECTORS			Unknown	<a href="#">link</a>			cisagov	2021-12-22
STERIS	AMSCO 600 MEDIUM STEAM STERILIZER			Unknown	<a href="#">link</a>			cisagov	2021-12-22
STERIS	AMSCO 7000 SERIES WASHER DISINFECTORS			Unknown	<a href="#">link</a>			cisagov	2021-12-22
STERIS	AMSCO CENTURY MEDIUM STEAM STERILIZER			Unknown	<a href="#">link</a>			cisagov	2021-12-22
STERIS	AMSCO CENTURY SMALL STEAM STERILIZER			Unknown	<a href="#">link</a>			cisagov	2021-12-22
STERIS	AMSCO EAGLE 3000 SERIES STAGE 3 STEAM STERILIZERS			Unknown	<a href="#">link</a>			cisagov	2021-12-22
STERIS	AMSCO EVOLUTION FLOOR LOADER STEAM STERILIZER			Unknown	<a href="#">link</a>			cisagov	2021-12-22

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
STERIS	AMSCO EVOLU- TION MEDIUM STEAM STERILIZER			Unknown	link			cisagov	2021-12-22
STERIS	Canexis 1.0			Unknown	link			cisagov	2021-12-22
STERIS	CELERITY HP INCUBATOR			Unknown	link			cisagov	2021-12-22
STERIS	CELERITY STEAM INCUBATOR			Unknown	link			cisagov	2021-12-22
STERIS	CER Optima			Unknown	link			cisagov	2021-12-22
STERIS	Clarity Software			Unknown	link			cisagov	2021-12-22
STERIS	Connect Software			Unknown	link			cisagov	2021-12-22
STERIS	ConnectAssure Technology			Unknown	link			cisagov	2021-12-22
STERIS	ConnectoHIS			Unknown	link			cisagov	2021-12-22
STERIS	CS-iQ Sterile Processing Workflow			Unknown	link			cisagov	2021-12-22
STERIS	DSD Edge			Unknown	link			cisagov	2021-12-22
STERIS	DSD-201,			Unknown	link			cisagov	2021-12-22
STERIS	EndoDry			Unknown	link			cisagov	2021-12-22
STERIS	Endora			Unknown	link			cisagov	2021-12-22
STERIS	Harmony iQ Integration Systems			Unknown	link			cisagov	2021-12-22
STERIS	Harmony iQ Perspectives Image Management System			Unknown	link			cisagov	2021-12-22
STERIS	HexaVue			Unknown	link			cisagov	2021-12-22
STERIS	HexaVue Integration System			Unknown	link			cisagov	2021-12-22
STERIS	IDSS Integration System			Unknown	link			cisagov	2021-12-22
STERIS	RapidAER			Unknown	link			cisagov	2021-12-22
STERIS	ReadyTracker			Unknown	link			cisagov	2021-12-22
STERIS	RealView Visual Workflow Management System			Unknown	link			cisagov	2021-12-22
STERIS	RELIANCE 444 WASHER DISINFECTOR			Unknown	link			cisagov	2021-12-22
STERIS	RELIANCE SYNERGY WASHER DISINFECTOR			Unknown	link			cisagov	2021-12-22
STERIS	RELIANCE VISION 1300 SERIES CART AND UTENSIL WASHER DISINFECTORS			Unknown	link			cisagov	2021-12-22

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
STERIS	RELIANCE VISION MULTI- CHAMBER WASHER DISINFECTOR			Unknown	link			cisagov	2021-12-22
STERIS	RELIANCE VISION SINGLE CHAMBER WASHER DISINFECTOR			Unknown	link			cisagov	2021-12-22
STERIS	Renatron			Unknown	link			cisagov	2021-12-22
STERIS	ScopeBuddy+			Unknown	link			cisagov	2021-12-22
STERIS	SecureCare ProConnect Technical Support Services			Unknown	link			cisagov	2021-12-22
STERIS	Situational Awareness for Everyone Display (S.A.F.E.)			Unknown	link			cisagov	2021-12-22
STERIS	SPM Surgical Asset Tracking Software			Unknown	link			cisagov	2021-12-22
STERIS	SYSTEM 1 endo LIQUID CHEMICAL STERILANT PROCESS- ING			Unknown	link			cisagov	2021-12-22
STERIS	SYSTEM V-PRO 1 LOW TEM- PERATURE STERILIZA- TION			Unknown	link			cisagov	2021-12-22
STERIS	SYSTEM V-PRO 1 PLUS LOW TEMPERA- TURE STERILIZA- TION			Unknown	link			cisagov	2021-12-22
STERIS	SYSTEM V-PRO MAX 2 LOW TEM- PERATURE STERILIZA- TION			Unknown	link			cisagov	2021-12-22
STERIS	SYSTEM V-PRO MAX LOW TEM- PERATURE STERILIZA- TION			Unknown	link			cisagov	2021-12-22
STERIS	SYSTEM V-PRO S2 LOW TEM- PERATURE STERILIZA- TION SYSTEM			Unknown	link			cisagov	2021-12-22

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
STERIS	VERIFY IN-CUBATOR FOR ASSERT SELF-CONTAINED BIOLOGICAL INDICATORS			Unknown	link			cisagov	2021-12-22
Sterling Order IBM				Unknown	link			cisagov	2022-01-12
Storagement				Unknown	link			cisagov	2022-01-12
StormShield				Unknown	link			cisagov	2022-01-12
StrangeBee				Unknown	link			cisagov	2022-01-12
TheHive & Cortex									
Stratodesk				Unknown	link			cisagov	2022-01-12
Strimzi				Unknown	link			cisagov	2022-01-12
Stripe				Unknown	link			cisagov	2022-01-12
Styra				Unknown	link			cisagov	2022-01-12
Sumologic				Unknown	link			cisagov	2022-01-12
SumoLogic				Unknown	link			cisagov	2022-01-12
Superna				Unknown	link			cisagov	2022-01-12
EYEGGLASS									
Suprema Inc				Unknown	link			cisagov	2022-01-12
SUSE				Unknown	link			cisagov	2022-01-12
Sweepwidget				Unknown	link			cisagov	2022-01-12
Swyx				Unknown	link			cisagov	2022-01-12
Synchro MSP				Unknown	link			cisagov	2022-01-12
Syncplify				Unknown	link			cisagov	2022-01-12
Synology				Unknown	link			cisagov	2022-01-12
Synopsys				Unknown	link			cisagov	2022-01-12
Syntevo				Unknown	link			cisagov	2022-01-12
SysAid				Unknown	link			cisagov	2022-01-12
Sysdig				Unknown	link			cisagov	2022-01-12
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	link			cisagov	2021-12-22
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	link			cisagov	2021-12-22
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	link			cisagov	2021-12-22
Tableau	Tableau Public Desktop Client	The following versions and lower: 2021.4		Affected	link			cisagov	2021-12-22

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Tableau	Tableau Reader	The following versions and lower: 2021.4		Affected	link			cisagov	2021-12-22
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	link			cisagov	2021-12-22
Talend				Unknown	link			cisagov	2022-01-12
Tanium	All			Not Affected	link	Tanium does not use Log4j.		cisagov	2021-12-21
TealiumIQ				Unknown	link			cisagov	2022-01-12
TeamPasswordManager				Unknown	link			cisagov	2022-01-12
Teamviewer				Unknown	link			cisagov	2022-01-12
Tech Software	OneAegis (f/k/a IRBManager)			Not Affected	link	OneAegis does not use Log4j.		cisagov	2021-12-15
Tech Software	SMART			Not Affected	link	SMART does not use Log4j.		cisagov	2021-12-15
Tech Software	Study Binders			Not Affected	link	Study Binders does not use Log4j.		cisagov	2021-12-15
TechSmith				Unknown	link			cisagov	2022-01-12
Telestream				Unknown	link			cisagov	2022-01-12
Tenable	Tenable.io / Nessus			Unknown	link	None of Tenable's products are running the version of Log4j vulnerable to CVE-2021-44228 or CVE-2021-45046 at this time		cisagov	2022-01-12
Thales	CADP/SafeNet Protect App (PA) - JCE			Unknown	link			cisagov	2021-12-17
Thales	CipherTrust Application Data Protection (CADP) – CAPLnet & Net Core			Unknown	link			cisagov	2021-12-17
Thales	CipherTrust Batch Data Transformation (BDT) 2.3			Unknown	link			cisagov	2021-12-17
Thales	CipherTrust Cloud Key Manager (CCKM)			Unknown	link			cisagov	2021-12-17
Thales	Appliance CipherTrust Cloud Key Manager (CCKM)			Unknown	link			cisagov	2021-12-17
Thales	Embedded CipherTrust Database Protection			Unknown	link			cisagov	2021-12-17

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Thales	CipherTrust Manager			Unknown	link			cisagov	2021-12-17
Thales	CipherTrust Transparent Encryption (CTE/VTE/CTE-U)			Unknown	link			cisagov	2021-12-17
Thales	CipherTrust Vaulted Tokenization (CT-V) / SafeNet Tokenization Manager			Unknown	link			cisagov	2021-12-17
Thales	CipherTrust Vaultless Tokenization (CTS, CT-VL)			Unknown	link			cisagov	2021-12-17
Thales	CipherTrust/SafeNet PDBCTL			Unknown	link			cisagov	2021-12-17
Thales	Crypto Command Center (CCC)			Unknown	link			cisagov	2021-12-17
Thales	Data Protection on Demand			Unknown	link			cisagov	2021-12-17
Thales	Data Security Manager (DSM)			Unknown	link			cisagov	2021-12-17
Thales	KeySecure			Unknown	link			cisagov	2021-12-17
Thales	Luna EFT			Unknown	link			cisagov	2021-12-17
Thales	Luna Network, PCIe, Luna USB HSM and backup devices			Unknown	link			cisagov	2021-12-17
Thales	Luna SP			Unknown	link			cisagov	2021-12-17
Thales	payShield			Unknown	link			cisagov	2021-12-17
Thales	Monitor			Unknown	link			cisagov	2021-12-17
Thales	ProtectServer HSMs			Unknown	link			cisagov	2021-12-17
Thales	SafeNet Authentication Client			Unknown	link			cisagov	2021-12-17
Thales	SafeNet eToken (all products)			Unknown	link			cisagov	2021-12-17
Thales	SafeNet IDPrime			Unknown	link			cisagov	2021-12-17
Thales	SafeNet Virtual IDPrime(all products)			Unknown	link			cisagov	2021-12-17
Thales	SafeNet LUKS			Unknown	link			cisagov	2021-12-17
Thales	SafeNet PKCS#11 and TDE			Unknown	link			cisagov	2021-12-17
Thales	SafeNet ProtectApp (PA) CAPI, .Net & Net Core			Unknown	link			cisagov	2021-12-17



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Thales	SafeNet ProtectDB (PDB)			Unknown	link			cisagov	2021-12-17
Thales	Safenet ProtectFile and ProtectFile-Fuse			Unknown	link			cisagov	2021-12-17
Thales	SafeNet ProtectV			Unknown	link			cisagov	2021-12-17
Thales	SafeNet SQL EKM			Unknown	link			cisagov	2021-12-17
Thales	SafeNet Transform Utility (TU)			Unknown	link			cisagov	2021-12-17
Thales	SafeNet Trusted Access (STA)			Unknown	link			cisagov	2021-12-17
Thales	SafeNet Vaultless			Unknown	link			cisagov	2021-12-17
Thales	Tokenization SAS on Prem (SPE/PCE)			Unknown	link			cisagov	2021-12-17
Thales	Sentinel Connect			Unknown	link			cisagov	2021-12-17
Thales	Sentinel EMS Enterprise aaS			Unknown	link			cisagov	2021-12-17
Thales	Sentinel EMS Enterprise OnPremise			Unknown	link			cisagov	2021-12-17
Thales	Sentinel Envelope			Unknown	link			cisagov	2021-12-17
Thales	Sentinel ESDaaS			Unknown	link			cisagov	2021-12-17
Thales	Sentinel HASP, Legacy dog, Maze, Hardlock			Unknown	link			cisagov	2021-12-17
Thales	Sentinel LDK EMS (LDK-EMS)			Unknown	link			cisagov	2021-12-17
Thales	Sentinel LDKaas (LDK-EMS)			Unknown	link			cisagov	2021-12-17
Thales	Sentinel Professional Services components (both Thales hosted & hosted on-premises by customers)			Unknown	link			cisagov	2021-12-17
Thales	Sentinel RMS			Unknown	link			cisagov	2021-12-17
Thales	Sentinel SCL			Unknown	link			cisagov	2021-12-17
Thales	Sentinel Superdog, SuperPro, UltraPro, SHK			Unknown	link			cisagov	2021-12-17
Thales	Sentinel Up			Unknown	link			cisagov	2021-12-17
Thales	Thales Data Platform (TDP)(DDC)			Unknown	link			cisagov	2021-12-17

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Thales	Thales payShield 10k			Unknown	link			cisagov	2021-12-17
Thales	Thales payShield 9000			Unknown	link			cisagov	2021-12-17
Thales	Thales payShield Manager			Unknown	link			cisagov	2021-12-17
Thales	Vormetirc Key Manager (VKM)			Unknown	link			cisagov	2021-12-17
Thales	Vormetric Application Encryption (VAE)			Unknown	link			cisagov	2021-12-17
Thales	Vormetric Protection for Terradata Database (VPTD)			Unknown	link			cisagov	2021-12-17
Thales	Vormetric Tokenization Server (VTS)			Unknown	link			cisagov	2021-12-22
Thermo Fisher Scientific Thermo-Calc	Thermo-Calc			Not Affected	link	Use the program as normal, Install the 2022a patch when available		cisagov	2021-12-22
Thermo-Calc	Thermo-Calc			Not Affected	link	Use the program as normal		cisagov	2021-12-22
Thermo-Calc	Thermo-Calc			Not Affected	link	Use the program as normal, delete the Log4j 2 files in the program installation if required, see advisory for instructions.		cisagov	2021-12-22
Thermo-Calc	Thermo-Calc			Not Affected	link	Use the program as normal		cisagov	2021-12-22

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Thomson Reuters	HighQ Appliance	<3.5		Affected	link	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.		cisagov	2021-12-20
ThreatLocker				Unknown	link			cisagov	2022-01-12
ThycoticCentralAccount Lifecycle Manager				Not Affected	link			cisagov	2021-12-10
ThycoticCentralCloud Suite				Not Affected	link			cisagov	2021-12-10
ThycoticCentralConnection Manager				Not Affected	link			cisagov	2021-12-10
ThycoticCentralDevOps				Not Affected	link			cisagov	2021-12-10
ThycoticCentralSecrets Vault				Not Affected	link			cisagov	2021-12-10
ThycoticCentralPassword Reset Server				Not Affected	link			cisagov	2021-12-10
ThycoticCentralPrivilege Manager				Not Affected	link			cisagov	2021-12-10
ThycoticCentralPrivileged Behavior Analytics				Not Affected	link			cisagov	2021-12-10
ThycoticCentralSecret Server				Not Affected	link			cisagov	2021-12-10
ThycoticCentralServer Suite				Not Affected	link			cisagov	2021-12-10
Tibco				Unknown	link			cisagov	2022-01-12
Top Gun Technology (TGT)				Unknown	link			cisagov	2022-01-12
TopDesk				Not Affected	link			cisagov	2021-12-20
Topicus	Topicus			Not Affected	link			cisagov	2021-12-20
Security	KeyHub			Not Affected	link			cisagov	2021-12-20
Topix				Unknown	link			cisagov	2022-01-12
Tosibox				Unknown	link			cisagov	2022-01-12
TPLink	Omega Controller	Linux/Windows(all)		Affected	link	Update is Beta. Reddit: overwrit-ten vulnerable log4j with 2.15 files as potential workaround. Though that should now be done with 2.16	Tp Community Link,Reddit Link	cisagov	2021-12-15
TrendMicro	All			Unknown	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Tricentis				Unknown	<a href="#">link</a>			cisagov	2022-01-12
Tosca									
Tridium				Unknown	<a href="#">link</a>	Document access requires authentication. CISA is not able to validate vulnerability status.		cisagov	2022-01-19
Trimble	eCognition	10.2.0 Build 4618		Affected		Remediation steps provided by Trimble		cisagov	2021-12-23
Tripp Lite	LX Platform devices (includes WEBCARDLX, WEBCARDLXMINI, SRCOOL-NETLX, SRCOOL-NET2LX and devices with pre-installed or embedded WEBCARDLX interfaces)			Unknown	<a href="#">link</a>			cisagov	2022-01-04
Tripp Lite	PowerAlert Local (PAL)			Unknown	<a href="#">link</a>	Some versions of PAL use log4j v1 which is NOT AFFECTED by the CVE-2021-44228 vulnerability.		cisagov	2022-01-04
Tripp Lite	PowerAlert Network Management System (PANMS)			Unknown	<a href="#">link</a>	Some versions of PAL use log4j v1 which is NOT AFFECTED by the CVE-2021-44228 vulnerability.		cisagov	2022-01-04
Tripp Lite	PowerAlert Network Shutdown Agent (PANSA)			Unknown	<a href="#">link</a>	Some versions of PANSA use log4j v1 which is NOT AFFECTED by the CVE-2021-44228 vulnerability.		cisagov	2022-01-04

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Tripp Lite	PowerAlertElement Manager (PAEM)	1.0.0		Affected	link	Tripp Lite will soon be issuing a patch in the form of PAEM 1.0.1 which will contain a patched version of Log4j2		cisagov	2022-01-04
Tripp Lite	SNMPWEBCARD, SRCOOL-NET, SRCOOL-NET2 and devices with pre-installed or embedded SNMPWEBCARD			Unknown	link			cisagov	2022-01-04
Tripp Lite	TLNETCARD and associated software			Unknown	link			cisagov	2022-01-04
Tripwire				Unknown	link			cisagov	2022-01-12
TrueNAS				Unknown	link			cisagov	2022-01-12
Tufin				Unknown	link			cisagov	2022-01-12
TYPO3				Unknown	link			cisagov	2022-01-12
Ubiquiti	UniFi Network Application	6.5.53 & lower versions		Affected	link			cisagov	2022-01-12
Ubiquiti	UniFi Network Controller	6.5.54 & lower versions		Affected	link		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	cisagov	2021-12-15
Ubuntu				Unknown	link			cisagov	2022-01-12
UiPath	InSights	20.10		Affected	link			cisagov	2021-12-15
Umbraco				Unknown	link			cisagov	2022-01-12
UniFlow				Unknown	link			cisagov	2022-01-12
Unify				Unknown	link			cisagov	2022-01-12
ATOS									
Unimus				Unknown	link			cisagov	2022-01-12
USSIGNAL				Unknown	link			cisagov	2022-01-12
MSP									
Varian	Acuity	All		Affected	link			cisagov	2021-12-22
Varian	ARIA Connect (Cloverleaf)			Not Affected	link			cisagov	2021-12-22
Varian	ARIA eDOC			Not Affected	link			cisagov	2021-12-22
Varian	ARIA oncology information system for Medical Oncology			Not Affected	link			cisagov	2021-12-22
Varian	ARIA oncology information system for Radiation Oncology			Not Affected	link			cisagov	2021-12-22

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Varian	ARIA Radiation Therapy Management System (RTM)			Not Affected	link			cisagov	2021-12-22
Varian	Bravos Console			Not Affected	link			cisagov	2021-12-22
Varian	Clinac	All		Affected	link			cisagov	2021-12-22
Varian	Cloud Planner			Not Affected	link			cisagov	2021-12-22
Varian	DITC	All		Affected	link			cisagov	2021-12-22
Varian	DoseLab			Not Affected	link			cisagov	2021-12-22
Varian	Eclipse treatment planning software			Not Affected	link			cisagov	2021-12-22
Varian	ePeerReview	All		Affected	link			cisagov	2021-12-22
Varian	Ethos			Not Affected	link			cisagov	2021-12-22
Varian	FullScale oncology IT solutions	All		Affected	link			cisagov	2021-12-22
Varian	Halcyon system	All		Affected	link			cisagov	2021-12-22
Varian	ICAP			Not Affected	link			cisagov	2021-12-22
Varian	Identify			Not Affected	link			cisagov	2021-12-22
Varian	Information Exchange Manager (IEM)			Not Affected	link			cisagov	2021-12-22
Varian	InSightive Analytics	All		Affected	link			cisagov	2021-12-22
Varian	Large Integrated Oncology Network (LION)			Not Affected	link			cisagov	2021-12-22
Varian	Mobius3D platform			Not Affected	link			cisagov	2021-12-22
Varian	PaaS			Not Affected	link			cisagov	2021-12-22
Varian	ProBeam			Not Affected	link			cisagov	2021-12-22
Varian	Qumulate			Not Affected	link			cisagov	2021-12-22
Varian	Real-time Position Management (RPM)			Not Affected	link			cisagov	2021-12-22
Varian	Respiratory Gating for Scanners (RGSC)			Not Affected	link			cisagov	2021-12-22
Varian	SmartConnect solution	All		Affected	link	See Knowledge Article: 000038850 on MyVarian		cisagov	2021-12-22

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Varian	SmartConnect solution Policy Server	All		Affected	link	See Knowledge Articles: 000038831 and 000038832 on MyVarian		cisagov	2021-12-22
Varian	TrueBeam radiotherapy system			Not Affected	link			cisagov	2021-12-22
Varian	UNIQUE system	All		Affected	link			cisagov	2021-12-22
Varian	Varian Authentication and Identity Server (VAIS)			Not Affected	link			cisagov	2021-12-22
Varian	Varian Managed Services Cloud	All		Affected	link			cisagov	2021-12-22
Varian	Varian Mobile App			Not Affected	link			cisagov	2021-12-22
Varian	VariSeed			Not Affected	link			cisagov	2021-12-22
Varian	Velocity			Not Affected	link			cisagov	2021-12-22
Varian	VitalBeam radiotherapy system			Not Affected	link			cisagov	2021-12-22
Varian	Vitesse			Not Affected	link			cisagov	2021-12-22
Varian	XMediusFax for ARIA oncology information system for Medical Oncology	All		Affected	link			cisagov	2021-12-22
Varian	XMediusFax for ARIA oncology information system for Radiation Oncology	All		Affected	link			cisagov	2021-12-22
VArmour				Unknown	link			cisagov	2022-01-12
Varnish Software				Unknown	link			cisagov	2022-01-12
Varonis				Unknown	link			cisagov	2022-01-12
Veeam				Unknown	link			cisagov	2022-01-12
Venafi				Unknown	link			cisagov	2022-01-12
Veritas				Unknown	link			cisagov	2022-01-12
NetBackup									
Vertica				Unknown	link			cisagov	2022-01-12
Video Insight Inc.	Video Insight			Not Affected	link	Video Insight is a part of Panasonic I-Pro.		cisagov	2022-01-19
Viso Trust				Unknown	link			cisagov	2022-01-12
VMware	API Portal for VMware Tanzu	1.x		Affected	link			cisagov	2021-12-12
VMware	App Metrics	2.x		Affected	link			cisagov	2021-12-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
VMware	Healthwatch for Tanzu Application Service	2.x, 1.x		Affected	link			cisagov	2021-12-12
VMware	Single Sign-On for VMware Tanzu Application Service	1.x		Affected	link			cisagov	2021-12-12
VMware	Spring Cloud Gateway for Kubernetes	1.x		Affected	link			cisagov	2021-12-12
VMware	Spring Cloud Gateway for VMware Tanzu	1.x		Affected	link			cisagov	2021-12-12
VMware	Spring Cloud Services for VMware Tanzu	3.x		Affected	link			cisagov	2021-12-12
VMware	vCenter Server - OVA	7.x, 6.7.x, 6.5.x		Affected	link	Workaround @ KB87081 (vmware.com)		cisagov	2021-12-17
VMware	vCenter Server - Windows	6.7.x, 6.5.x		Affected	link	Workaround @ KB87096 (vmware.com)		cisagov	2021-12-17
VMware	VMware Carbon Black Cloud Workload Appliance	1.x		Affected	link			cisagov	2021-12-12
VMware	VMware Carbon Black EDR Server	7.x, 6.x		Affected	link			cisagov	2021-12-12
VMware	VMware Cloud Foundation	4.x, 3.x		Affected	link			cisagov	2021-12-12
VMware	VMware HCX	4.x, 3.x		Affected	link			cisagov	2021-12-12
VMware	VMware Horizon	8.x, 7.x		Affected	link		VMware KB 87073 (vmware.com)	cisagov	2021-12-17
VMware	VMware Horizon Cloud Connector	1.x, 2.x		Affected	link			cisagov	2021-12-12
VMware	VMware Horizon DaaS	9.1.x, 9.0.x		Affected	link			cisagov	2021-12-12
VMware	VMware Identity Manager	3.3.x		Affected	link			cisagov	2021-12-12
VMware	VMware NSX-T Data Centern	3.x, 2.x		Affected	link			cisagov	2021-12-12
VMware	VMware Site Recovery Manager	8.x		Affected	link			cisagov	2021-12-12
VMware	VMware Tanzu Application Service for VMs	2.x		Affected	link			cisagov	2021-12-12
VMware	VMware Tanzu GemFire	9.x, 8.x		Affected	link			cisagov	2021-12-12



Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
VMware	VMware Tanzu Greenplum	6.x		Affected	link			cisagov	2021-12-12
VMware	VMware Tanzu Kubernetes Grid	1.x		Affected	link			cisagov	2021-12-12
VMware	VMware Tanzu Integrated Edition	3.x, 2.x		Affected	link			cisagov	2021-12-12
VMware	VMware Tanzu Observability by Wavefront Nozzle	2.x		Affected	link			cisagov	2021-12-12
VMware	VMware Tanzu Operations Manager	2.x, 1.x		Affected	link			cisagov	2021-12-12
VMware	VMware Tanzu SQL with MySQL for VMs	2.x, 1.x		Affected	link			cisagov	2021-12-12
VMware	VMware Telco Cloud Automation	21.x, 20.x, 3.x		Affected	link			cisagov	2021-12-12
VMware	VMware Unified Access Gateway	1.x		Affected	link			cisagov	2021-12-12
VMware	VMware vCenter Cloud Gateway	8.x, 7.x		Affected	link			cisagov	2021-12-12
VMware	VMware vRealize Automation	8.x		Affected	link			cisagov	2021-12-12
VMware	VMware vRealize Lifecycle Manager	8.x		Affected	link			cisagov	2021-12-12
VMware	VMware vRealize Log Insight	8.x		Affected	link			cisagov	2021-12-12
VMware	VMware vRealize Operations	Any		Affected	link			cisagov	2021-12-12
VMware	VMware vRealize Operations Cloud Proxy	8.x, 7.x		Affected	link			cisagov	2021-12-12
VMware	VMware vRealize Orchestrator	21.x, 20.10.x		Affected	link			cisagov	2021-12-12
VMware	VMware Workspace ONE Access Connector (VMware Identity Manager Connector)	21.x, 20.10.x, 19.03.0.1		Affected	link			cisagov	2021-12-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
VTScada	All			Not Affected	link	Java is not utilized within VTScada software, and thus our users are unaffected.		cisagov	2022-01-17
Vyaire				Unknown	link			cisagov	2021-12-22
WAGO	WAGO Smart Script	4.2.x < 4.8.1.3		Affected	link			cisagov	2021-12-17
Wallarm				Unknown	link			cisagov	2022-01-12
Wasp Barcode technologies				Unknown	link			cisagov	2022-01-12
WatchGuard	Secplicity			Unknown	link			cisagov	2022-01-12
Western Digital				Unknown	link			cisagov	2022-01-12
WIBU Systems	CodeMeter Cloud Lite	2.2 and prior		Affected	link			cisagov	2021-12-22
WIBU Systems	CodeMeter Keyring for TIA Portal	1.30 and prior		Affected	link	Only the Password Manager is affected		cisagov	2021-12-22
WindRiver				Unknown	link			cisagov	2022-01-12
WireShark				Unknown	link			cisagov	2022-01-12
Wistia				Unknown	link			cisagov	2022-01-12
WitFoo				Unknown	link			cisagov	2022-01-12
WordPress				Unknown	link			cisagov	2022-01-12
Worksphere				Unknown	link			cisagov	2022-01-12
Wowza				Unknown	link			cisagov	2022-01-12
WSO2	WSO2 Enterprise Integrator	6.1.0 and above		Affected	link	A temporary mitigation is available while vendor works on update		cisagov	2022-01-12
XCP-ng				Unknown	link			cisagov	2022-01-12
XenForo				Unknown	link			cisagov	2022-01-12
Xerox				Unknown	link			cisagov	2022-01-12
XPertDoc				Unknown	link			cisagov	2022-01-12
XPLG				Unknown	link			cisagov	2022-01-12
XWIKI				Unknown	link			cisagov	2022-01-12
Xylem	Aquataalk			Unknown	link			cisagov	2021-12-22
Xylem	Avensor			Unknown	link			cisagov	2021-12-22
Xylem	Configuration change complete			Unknown	link			cisagov	2021-12-22
Xylem	Sensus Analytics			Unknown	link			cisagov	2021-12-22
Xylem	Sensus Automation Control Configuration change complete			Unknown	link			cisagov	2021-12-22
Xylem	Sensus Cathodic Protection Mitigation in process Mitigation in process			Unknown	link			cisagov	2021-12-22

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Xylem	Sensus FieldLogic LogServer			Unknown	link			cisagov	2021-12-22
Xylem	Sensus Lighting Control			Unknown	link			cisagov	2021-12-22
Xylem	Sensus NetMetrics Configuration change complete			Unknown	link			cisagov	2021-12-22
Xylem	Sensus RNI On Prem	4.7 through 4.10, 4.4 through 4.6, 4.2		Affected	link			cisagov	2021-12-22
Xylem	Sensus RNI Saas	4.7 through 4.10, 4.4 through 4.6, 4.2		Affected	link			cisagov	2021-12-22
Xylem	Sensus SCS			Unknown	link			cisagov	2021-12-22
Xylem	Smart Irrigation			Unknown	link			cisagov	2021-12-22
Xylem	Water Loss Management (Visenti)			Unknown	link			cisagov	2021-12-22
Xylem	Xylem Cloud			Unknown	link			cisagov	2021-12-22
Xylem	Xylem Edge Gateway (xGW)			Unknown	link			cisagov	2021-12-22
Yellowbrick				Unknown	link			cisagov	2022-01-12
YellowFin				Unknown	link			cisagov	2022-01-12
YOKOGAWA				Unknown	link			cisagov	2021-12-22
YSoft				Unknown	link			cisagov	2022-01-12
SAFEQ									
Zabbix				Unknown	link			cisagov	2022-01-12
ZAMMAD				Unknown	link			cisagov	2022-01-12
Zaproxy				Unknown	link			cisagov	2022-01-12
Zebra				Unknown	link			cisagov	2022-01-12
Zendesk	All Products	All Versions		Affected	link	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.		cisagov	2021-12-13
Zenoss				Unknown	link			cisagov	2022-01-12
Zentera	CoIP Access			Not Affected	link			cisagov	2021-12-17
Systems, Inc.	Platform								
Zerto				Unknown	link			cisagov	2022-01-12
Zesty				Unknown	link			cisagov	2022-01-12
Zimbra				Unknown	link			cisagov	2022-01-12
Zix				Unknown	link			cisagov	2021-12-16
Zoom				Unknown	link			cisagov	2022-01-12
ZPE systems Inc				Unknown	link			cisagov	2022-01-12

Vendor	Product	Affected Versions	Patched Versions	Status	Vendor Links	Notes	References	Reporter	Last Updated
Zscaler	See Link (Multiple Products)			Unknown	link			cisagov	2021-12-15
Zyxel				Unknown	link			cisagov	2022-01-12
Zyxel	Security Firewall/Gateways			Not Affected	link			cisagov	2021-12-14