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

## Status Descriptions

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

## Software List

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

- Kevin Beaumont SwitHak

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Password	All products		Not affected		1Password statement			12/23/2021
'n					2n Advisory Link			
CX					3CX Community			
					Thread Link			10/17/1000
BM Health	CGS		Affected	Unknown	CGS: Log4j Software	This		12/15/2021
Information					Update(login required)	advisory is		
Systems						available to		
						customer		
						only and		
						has not		
						been		
						reviewed		
						by CISA.		
7-Zip					7Zip Discussion Link			
ABB	4 D D D	1000	1.00		ABB Link			
ABB	ABB Remote Service	ABB Remote Platform (RAP)	Affected		Details are shared with active subscribers			
ABB	AlarmInsight	AlarmInsight KPI	Under					
	Cloud	Dashboards 1.0.0	Investigation					
ABB	B&R Products	See Vendor Advisory			BR-Automation			
					Advisory			
Abbott					Abbott Advisory Link			12/15/2021
Abnormal	Abnormal		Not affected		Abnormal Blog			
Security	Security				A 11 A 1			
Accellence					Accellence Article			

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
AFHCAN Global LLC	AFHCANcart	8.0.7 - 8.4.3	Not Affected		https://afhcan.org/			
AFHCAN	AFHCANweb	8.0.7 - 8.4.3	Not Affected		support.aspx https://afhcan.org/			
Global LLC AFHCAN Global LLC	AFHCANmobile	8.0.7 - 8.4.3	Not Affected		support.aspx https://afhcan.org/ support.aspx			
AFHCAN Global LLC Agilysys	AFHCANupdate	8.0.7 - 8.4.3	Not Affected		https://afhcan.org/ support.aspx Agilysys Link			
Advanced Systems Concepts (formally Jscape)	Active MFT		Not Affected	No	Log4J Vulnerabilty	This advisory is available to customers		12/14/2021
Advanced	MFT Server		Not Affected	No	Log4J Vulnerabilty	only and has not been reviewed by CISA This		12/14/2021
Systems Concepts (formally Jscape)						advisory is available to customers only and has not been reviewed		
Advanced Systems Concepts (formally Jscape)	MFT Gateway		Not Affected	No	Log4J Vulnerabilty	by CISA This advisory is available to customers only and has not been reviewed by CISA		12/14/2021
Advanced Systems Concepts (formally Jscape)	MFT		Not Affected	No	Log4J Vulnerabilty	This advisory is available to customers only and has not been reviewed by CISA		12/14/2021
Akamai	SIEM Splunk Connector	All	Affected	Yes	Akamai SIEM Integration	v1.4.11 is the new recommen- dation for mitigation of log4j vulnerabilitie	29	12/15/2021
Alcatel Alertus Alexion Alfresco AlienVault Alphatron Medical					Alcatel Link Alertus Article Link Alexion Blog Post Alfresco Blog Post AlienVault Article Link Alphatron Medical Website	vanciabilitie		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Vendor Amazon	AWS	Version(s) Linux 1,2	Status  Not Affected	No No	Vendor Link	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-	Last Updated 12/15/2021
Amazon	AWS API	All	Fixed		Amazon AWS Link	gp2	12/20/2021
Amazon	Gateway AWS CloudHSM	< 3.4.1.	Affected		Apache Log4j2 Security Bulletin (CVE-2021-44228) (amazon.com)		
Amazon	AWS Connect	All	Fixed		Vendor Link	Vendors recommend evaluating components of the envi- ronment outside of the Amazon Connect service boundary, which may require sepa- rate/additional customer mitigation	12/23/2021
Amazon	AWS Lambda	Unknown	Affected	Yes	Apache Log4j2 Security Bulletin (CVE-2021-44228) (amazon.com)	muganon	
Amazon	EC2	Amazon Linux 1 & 2	Not Affected		(amazon.com) Apache Log4j2 Security Bulletin (CVE-2021-44228) (amazon.com)		12/15/2021
Amazon	AWS DynamoDB	Unknown	Fixed		Update for Apache Log4j2 Issue (CVE-2021-44228)		12/17/2021

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Amazon	AWS EKS, ECS,		Affected	Yes	Update for Apache	To help		12/16/2021
	Fargate				Log4j2 Issue	mitigate		
					(CVE-2021-44228)	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		
						Log 4J2		
						library in		
						customers' containers.		
						These		
						updates		
						are		
						available as an		
						Amazon		
						Linux		
						package		
						for Amazon		
						ECS ECS		
						customers,		
						as a Dae-		
						monSet for		
						Kuber- netes users		
						on AWS,		
						and will		
						be in		
						$\begin{array}{c} \text{supported} \\ \text{AWS} \end{array}$		
						AWS Fargate		
						platform		
						versions		
				6				

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Amazon	AWS ELB	Unknown	Fixed		Update for Apache			12/16/2021
					Log4j2 Issue (CVE-2021-44228)			
Amazon	AWS Kinesis	Unknown	Affected	Yes	Update for Apache	We are		12/14/2021
	Data Stream				Log4j2 Issue	actively		,,
					(CVE-2021-44228)	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		
						recom-		
						mend that all KCL		
						version 1.x		
						customers		
						upgrade to		
						KCL		
						version		
						1.14.5 (or higher)		
Amazon	OpenSearch	Unknown	Affected	Yes	Apache Log4j2 Security	mgner)		
					Bulletin			
					(CVE-2021-44228)			
					(amazon.com),			
			Not affected		(R20211203-P2) Amazon Translate	Service not		
Amazon	Translate		not anected		Amazon Hansiate	identified		
Amazon	Translate							
Amazon	Translate					on AWS		
Amazon	Translate					on AWS $Log4j$		
Amazon	Translate					on AWS Log4j Security		
			Not Affortal		AMD Advisory Link	on AWS Log4j Security Bulletin		19/99/9091
Amazon  AMD	Translate All		Not Affected		AMD Advisory Link	on AWS Log4j Security Bulletin Currently,		12/22/2021
			Not Affected		AMD Advisory Link	on AWS Log4j Security Bulletin Currently, no AMD		12/22/2021
			Not Affected		AMD Advisory Link	on AWS Log4j Security Bulletin Currently, no AMD products have been		12/22/2021
			Not Affected		AMD Advisory Link	on AWS Log4j Security Bulletin Currently, no AMD products have been identified		12/22/2021
			Not Affected		AMD Advisory Link	on AWS Log4j Security Bulletin Currently, no AMD products have been identified as affected.		12/22/2021
			Not Affected		AMD Advisory Link	on AWS Log4j Security Bulletin Currently, no AMD products have been identified as affected. AMD is		12/22/2021
			Not Affected		AMD Advisory Link	on AWS Log4j Security Bulletin Currently, no AMD products have been identified as affected.		12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Anaconda	Anaconda	4.10.3	Not Affected		https://docs.conda.io/ projects/conda/en/ latest/index html			12/21/2021
Apache	ActiveMQ Artemis	All	Not Affected	Yes	latest/index.html ApacheMQ - Update on CVE-2021-4428	Artemis does not use Log4j for logging. However, Log4j 1.2.17 is included in the Hawtio-based web console application archive (i.e. web/console. war/WEB-INF/lib). Although this version of Log4j is not impacted by CVE-2021-44228 future versions of Artemis will be updated so that the Log4j jar is no longer included in the web console application archive. See ARTEMIS-3612 for more informore informore information in the web console application archive.		12/21/2021
Apache	Airflow		Not affected		Apache Airflow	mation on that task. Airflow is		
Tipuono	THIIOW		1100 anocood		ripuono rimnow	written in Python		

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Apache	Druid	< druid 0.22.0	Affected	Yes	Release druid-0.22.1			12/12/2021
Apache	Druid Flink	< druid 0.22.0 < 1.14.2, 1.13.5, 1.12.7, 1.11.6	Affected Fixed	Yes	Release druid-0.22.1 · apache/druid · GitHub Apache Flink: Advise on Apache Log4j Zero Day (CVE-2021-44228)	To clarify and avoid confusion: The 1.14.1 / 1.13.4 / 1.12.6 / 1.11.5 releases, which were supposed to only contain a Log4j upgrade to 2.15.0, were skipped because CVE-2021-45046 was discovered during the release publication. The new 1.14.2 / 1.13.5 / 1.12.7 / 1.11.6 releases include a version upgrade for Log4j to version 2.16.0 to address CVE-2021-44228 and CVE-2021-4428 and CVE-2021-	https://flink.apache.org/news/2021/12/16/log4j-patch-releases.html	12/12/2021
Apache	Kafka	All	Not Affected	No	Kafka Apache List	The current DB lists Apache Kafka as impacted. Apache Kafka uses Log4jv1,		12/14/2021
Apache	Kafka	Unknown	Affected	No	Log4j – Apache Log4j Security Vulnerabilities	not v2. Only vulnerable in certain	n(c)	
Apache	Log4j	< 2.15.0	Affected	Yes	Log4j – Apache Log4j Security Vulnerabilities	configuration	п(э)	
Apache	Solr	7.4.0 to 7.7.3, 8.0.0 to 8.11.0	Fixed	Yes	Apache Solr Security	Update to 8.11.1 or apply fixes as described in Solr security advisory	Apache Solr 8.11.1 downloads	12/16/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Apache	Struts 2	Versions before 2.5.28.1	Fixed (See	Yes	Apache Struts	The	Apache Struts Release Downloads	12/21/2021
			Notes)		Announcements	Apache		
						Struts		
						group is		
						pleased to		
						announce		
						that Struts		
						2.5.28.1  is		
						available		
						as a		
						${\rm ``General'}$		
						Availabil-		
						ity"		
						release.		
						The GA		
						designa-		
						tion is our		
						highest		
						quality		
						grade.		
						This		
						release		
						addresses		
						Log4j vul-		
						nerability CVE-2021-		
						45046 by		
						using the		
						latest		
						Log4j		
						2.12.2		
						version		
						(Java 1.7		
						compatible		

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
pache	Tomcat	9.0.x	Not Affected		Apache Tomcat Security	Apache		12/21/2021
			(See Notes)		Notes	Tomcat		
						9.0.x has		
						no depen-		
						dency on		
						any		
						version of		
						log4j. Web		
						applica- tions		
						deployed		
						on Apache		
						Tomcat		
						may have		
						a depen-		
						dency on		
						log4j. You		
						should		
						seek		
						support		
						from the		
						applica-		
						tion		
						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		
						configura-		
						tion 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 vul-		
						nerability.		
						In most		
						cases,		
						disabling		
						the prob-		
						lematic		
						feature		
						will be the		
						simplest		
						solution.		
						Exactly		
						how to do		
					10	that		
					12	depends		
						on the		
						exact		
						version of		
						log4j 2.x		
						being used.		
						Details are		
						provided		
						on the		
						14: 0		
						log4j 2.x		
						security page		

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Arcserve	StorageCraft OneXafe	All	Not Affected	No	https://support. storagecraft.com/s/ article/Log4J-Update		https://support.storagecraft.com/s/question/0D51R000089NnT3SAK/does-storagecraft-have-a-publicly-available-response-to-the-log4j-vulnerability-is-there-a-reference-for-any-findings-negative-positive-the-company-has-in-their-investigations-it-seems-it-would-greatly-benefit-support-and-customers-both?language=en_US	12/14/2021
ArcticWolf Arduino Ariba Arista Aruba Networks Ataccama Atera					ArcticWolf Blog Post Arduino Support Link Ariba Annoucement Arista Advisory Notice Aruba Networks Notification Ataccama Link Atera Link		both: language—en05	
Atlassian	Bamboo Server & Data Center	All	Not Affected		Multiple Products Security Advisory - Log4j Vulnerable To Remote Code Execution - CVE-2021-44228	This product may be affected by a related but lower severity vulnerability if running in a specific nondefault configuration	1.	
Atlassian	Bitbucket Server & Data Center	All	Affected	Yes	Multiple Products Security Advisory - Log4j Vulnerable To Remote Code Execution - CVE-2021-44228	This product is not vulnerable to remote code execution but may leak information due to the bundled Elastic-search component being vulnerable.		
Atlassian	Confluence Server & Data Center	All	Not Affected		Multiple Products Security Advisory - Log4j Vulnerable To Remote Code Execution - CVE-2021-44228	rhis product may be affected by a related but lower severity vulnerability if running in a specific non- default configuration	1.	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Update
Atlassian	Crowd Server & Data Center	All	Not Affected		Multiple Products Security Advisory - Log4j Vulnerable To Remote Code Execution - CVE-2021-44228	a related but lower severity		
Atlassian	Crucible	All	Not Affected		Multiple Products Security Advisory - Log4j Vulnerable To Remote Code Execution - CVE-2021-44228	vulnerability if running in a specific non- default configuration This product may be affected by a related but lower	1.	
Atlassian	Fisheye	All	Not Affected		Multiple Products	severity vulnerability if running in a specific non- default configuration This	1.	
					Security Advisory - Log4j Vulnerable To Remote Code Execution - CVE-2021-44228	product may be affected by a related but lower severity vulnerabil- ity if running in a specific non-		
Atlassian	Jira Server & Data Center	All	Not Affected		Multiple Products Security Advisory - Log4j Vulnerable To Remote Code Execution - CVE-2021-44228	default configuration This product may be affected by a related but lower severity vulnerability if running in a specific non-	1.	
Attivo networks AudioCodes					Attivo Networks Advisory AudioCodes Link	default configuration	1.	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Autodesk	110000	, croion(s)	Under	орашо пуаналю	Autodesk Article Link	Autodesk	Julior recreditions	12/21/2021
11uvouesk			Investigation		Autouesk Afticle Lilik	is		12/21/2021
			mvcongation			continuing		
						to perform		
						a thorough		
						investiga-		
						tion in		
						relation to the		
						recently		
						discovered		
						Apache		
						Log4j		
						security		
						vulnerabil- ities. We		
						continue		
						to		
						implement		
						several		
						mitigating		
						factors for		
						$\begin{array}{c} \mathrm{our} \\ \mathrm{products} \end{array}$		
						including		
						patching,		
						network		
						firewall		
						blocks,		
						${ m and}$ ${ m updated}$		
						detection		
						signatures		
						to reduce		
						the threat		
						of this vul-		
						nerability and		
						enhance		
						our ability		
						to quickly		
						respond to		
						potential		
						malicious		
						activity. We have		
						not		
						identified		
						any com-		
						promised		
						systems in		
						${ m the} \ { m Autodesk}$		
						environ-		
						ment due		
						to this vul-		
						nerability,		
						at this		
						time. This is an		
						ongoing in-		
						vestigation		
						and we		
						will		
						provide		
						updates on		
						the Autodesk		
						Trust		
						Center as		
					17	we learn		

more.

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Avaya	Avaya Aura® Web Gateway	3.11[P], 3.8.1[P], 3.8[P], 3.9.1 [P], 3.9[P]	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products			12/14/2021
Avaya	Avaya Breeze $^{\mathrm{TM}}$	3.7, 3.8, 3.8.1	Affected	No	Avaya Product Security Apache Log4J Vulnerability - Impact for Avaya products			12/14/2021
Avaya	Avaya Contact Center Select	7.0.2, 7.0.3, 7.1, 7.1.1, 7.1.2	Affected	No	Avaya Product Security Apache Log4J Vulnerability - Impact			12/14/2021
Avaya	Avaya CRM Connector -	2.2	Affected	No	for Avaya products Avaya Product Security Apache Log4J Vulnerability - Impact			12/14/2021
Avaya	Connected Desktop Avaya Device	3.1.22	Affected	No	for Avaya products Avaya Product Security Apache Log4J			12/14/2021
. I Trug u	Enablement Service	5.1. <u>-2</u>	Timoood		Vulnerability - Impact for Avaya products Avaya Product Security			12/11/2021
Avaya	Avaya Meetings	9.1.10, 9.1.11, 9.1.12	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products			12/14/2021
Avaya	Avaya one cloud private -UCaaS - Mid Market		Affected	No	Avaya Product Security Apache Log4J Vulnerability - Impact for Avaya products			12/14/2021
Avaya	Aura Avaya OneCloud- Private	2	Affected	No	Avaya Product Security Apache Log4J Vulnerability - Impact for Avaya products			12/14/2021
Avaya	Avaya Session Border Controller for	8.0.1, 8.1, 8.1.1, 8.1.2, 8.1.3	Affected	Yes	Avaya Product Security Apache Log4J Vulnerability - Impact for Avaya products		PSN020554u	12/14/2021
Avaya	Enterprise Avaya Social Media Hub		Affected	No	Avaya Products  Avaya Product Security  Apache Log4J  Vulnerability - Impact  for Avaya products			12/14/2021
Avaya	Avaya Workforce Engagement	5.3	Affected	No	Avaya Products  Avaya Product Security  Apache Log4J  Vulnerability - Impact  for Avaya products			12/14/2021
Avaya	Business Rules Engine	3.4, 3.5, 3.6, 3.7	Affected	No	Avaya Product Security Apache Log4J Vulnerability - Impact for Avaya products			12/14/2021
Avaya	Callback Assist	5, 5.0.1	Affected	No	Avaya Products  Avaya Product Security  Apache Log4J  Vulnerability - Impact  for Avaya products			12/14/2021
Avaya	Control Manager	9.0.2, 9.0.2.1	Affected	No	Avaya products  Avaya Product Security  Apache Log4J  Vulnerability - Impact  for Avaya products			12/14/2021
Avaya	Device Enrollment Service	3.1	Affected	No	Avaya Product Security Apache Log4J Vulnerability - Impact for Avaya products			12/14/2021
Avaya	$\begin{array}{c} \text{Equinox}^{\text{TM}} \\ \text{Conferencing} \end{array}$	9.1.2	Affected	No	Avaya Product Security Apache Log4J Vulnerability - Impact for Avaya products			12/14/2021
Avaya	Interaction Center	7.3.9	Affected	No	Avaya products  Avaya Product Security  Apache Log4J  Vulnerability - Impact  for Avaya products			12/14/2021

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
BD	BD		Not Affected	No	BD Advisory Link			12/20/2021
	$HealthSight^{TM}$							
	Diversion							
	Management							
BD	BD		Not Affected	No	BD Advisory Link			12/20/2021
	$HealthSight^{TM}$							
	Infection							
DD	Advisor		N . A.C 1	N.	DD 41: T: 1			12 /22 /2221
BD	BD		Not Affected	No	BD Advisory Link			12/20/2021
	$ m HealthSight^{TM}$							
	Inventory							
	Optimization							
DD	Analytics BD		Not Affected	Ma	DD Adminorus Link			19 /90 /9091
BD	$ m HealthSight^{TM}$		Not Affected	NO	BD Advisory Link			12/20/2021
	Medication							
	Safety							
BD	BD Knowledge		Not Affected	No	BD Advisory Link			12/20/2021
ענו	Portal for		1100 Affected	110	DD MANISOLY LILL			12/20/2021
	Infusion							
	Technologies							
BD	BD Knowledge		Not Affected	No	BD Advisory Link			12/20/2021
DD	Portal for		1100 IIIIococa	110	BB Havisory Emin			12/20/2021
	Medication							
	Technologies							
BD	BD Knowledge		Not Affected	No	BD Advisory Link			12/20/2021
	Portal for BD							,,
	$Pyxis^{TM}$ Supply							
BD	$\mathrm{BD}\ \mathrm{Synapsys^{TM}}$		Not Affected	No	BD Advisory Link			12/20/2021
	Informatics							, ,
	Solution							
BD	$BD Veritor^{TM}$		Not Affected	No	BD Advisory Link			12/20/2021
	COVID At							
	Home Solution							
	Cloud							
Beckman			Under		Beckman Coulter			12/20/2021
Coulter			Investigation		Advisory Link			
Beijer	acirro+		Not Affected		Beijer Electronics			12/22/2021
Electronics					Advisory Link			10.100.1000
Beijer	BFI frequency		Not Affected		Beijer Electronics			12/22/2021
Electronics	inverters		NT / A (" / 1		Advisory Link			10/00/0001
Beijer	BSD servo		Not Affected		Beijer Electronics			12/22/2021
Electronics	drives ClaudVPN		Not Affected		Advisory Link			19 /99 /9091
Beijer Electronics	CloudVPN		Not Affected		Beijer Electronics Advisory Link			12/22/2021
Beijer	FnIO-G and M		Not Affected		Beijer Electronics			12/22/2021
Electronics	Distributed IO		Not Affected		Advisory Link			12/22/2021
Beijer	iX Developer		Not Affected		Beijer Electronics			12/22/2021
Electronics	111 Developer		1,00 Imcood		Advisory Link			12/22/2021
Beijer	Nexto modular		Not Affected		Beijer Electronics			12/22/2021
Electronics	PLC				Advisory Link			, , ====
Beijer	Nexto Xpress		Not Affected		Beijer Electronics			12/22/2021
Electronics	compact				Advisory Link			, ,
	controller				·			
Beijer	WARP		Not Affected		Beijer Electronics			12/22/2021
Electronics	Engineering				Advisory Link			, ,
	Studio				v			
			TT 1		D: - M A			10/00/0001
BioMerieux			Under		BioMerieux Advisory			12/22/2021
BioMerieux Bender			Under Investigation		Link Bender Link			12/22/2021

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

Vendor	Product Version(s)	Status Update Available	Vendor Link Notes Other References	Last Updated
BMC	BMC Helix	Under	BMC Security Advisory	
	Client	Investigation	for CVE-2021-44228	
	Management		Log4Shell Vulnerability -	
			Blogs & Documents -	
			BMC Community	
BMC	BMC Helix	Under	BMC Security Advisory	
	Cloud Cost	Investigation	for CVE-2021-44228	
			Log4Shell Vulnerability -	
			Blogs & Documents -	
DMC	DMC II I:	TT 1	BMC Community	
BMC	BMC Helix Cloud Security	Under	BMC Security Advisory for CVE-2021-44228	
	Cloud Security	Investigation	Log4Shell Vulnerability -	
			Blogs & Documents -	
			BMC Community	
BMC	BMC Helix	Under	BMC Security Advisory	
DMC	CMDB	Investigation	for CVE-2021-44228	
	ONDB	111100015401011	Log4Shell Vulnerability -	
			Blogs & Documents -	
			BMC Community	
BMC	BMC Helix	Under	BMC Security Advisory	
	Continuous	Investigation	for CVE-2021-44228	
	Optimization		Log4Shell Vulnerability -	
	•		Blogs & Documents -	
			BMC Community	
BMC	BMC Helix	$\operatorname{Under}$	BMC Security Advisory	
	Control-M	Investigation	for CVE-2021-44228	
			Log4Shell Vulnerability -	
			Blogs & Documents -	
			BMC Community	
BMC	BMC Helix	Under	BMC Security Advisory	
	Digital	Investigation	for CVE-2021-44228	
	Workplace		Log4Shell Vulnerability -	
			Blogs & Documents -	
DMC	DMC II-li	II. 1	BMC Community	
BMC	BMC Helix	Under	BMC Security Advisory	
	Discovery	Investigation	for CVE-2021-44228 Log4Shell Vulnerability -	
			Blogs & Documents -	
			BMC Community	
BMC	BMC Helix	Under	BMC Security Advisory	
<b>D</b> 1110	ITSM	Investigation	for CVE-2021-44228	
			Log4Shell Vulnerability -	
			Blogs & Documents -	
			BMC Community	
BMC	BMC Helix	Under	BMC Security Advisory	
	Knowledge	Investigation	for CVE-2021-44228	
	Management		Log4Shell Vulnerability -	
			Blogs & Documents -	
			BMC Community	
BMC	BMC Helix	Under	BMC Security Advisory	
	Operations	Investigation	for CVE-2021-44228	
	Management		Log4Shell Vulnerability -	
	with AIOps		Blogs & Documents -	
BMC	BMC Helix	Under	BMC Community BMC Security Advisory	
BMC	Platform		BMC Security Advisory for CVE-2021-44228	
	FIRMOTHI	Investigation	Log4Shell Vulnerability -	
			Blogs & Documents -	
			BMC Community	
BMC	BMC Helix	Under	BMC Security Advisory	
21110	platform	Investigation	for CVE-2021-44228	
	Protection	111,00018001011	Log4Shell Vulnerability -	
			Blogs & Documents -	
			BMC Community	

Vendor	Product Version(s)	Status Update Available	Vendor Link Notes Other References	Last Updated
BMC	BMC Helix	Under	BMC Security Advisory	
	Remediate	Investigation	for CVE-2021-44228 Log4Shell Vulnerability -	
			Blogs & Documents -	
			BMC Community	
BMC	BMC Helix	Under	BMC Security Advisory	
	Remediate	Investigation	for CVE-2021-44228	
			Log4Shell Vulnerability -	
			Blogs & Documents - BMC Community	
BMC	BMC Helix	Under	BMC Security Advisory	
	Remedyforce	Investigation	for CVE-2021-44228	
			Log4Shell Vulnerability -	
			Blogs & Documents -	
BMC	BMC Helix	$\operatorname{Under}$	BMC Community BMC Security Advisory	
BMC	Virtual Agent	Investigation	for CVE-2021-44228	
			Log4Shell Vulnerability -	
			Blogs & Documents -	
DMG		***	BMC Community	
BMC	Cloud Lifecycle Management	Under Investigation	BMC Security Advisory for CVE-2021-44228	
	Management	investigation	Log4Shell Vulnerability -	
			Blogs & Documents -	
			BMC Community	
BMC	Control-M	Under	BMC Security Advisory	
		Investigation	for CVE-2021-44228	
			Log4Shell Vulnerability - Blogs & Documents -	
			BMC Community	
BMC	Footprints	Under	BMC Security Advisory	
		Investigation	for CVE-2021-44228	
			Log4Shell Vulnerability -	
			Blogs & Documents - BMC Community	
BMC	MainView	$\operatorname{Under}$	BMC Security Advisory	
21.10	Middleware	Investigation	for CVE-2021-44228	
	Administrator		Log4Shell Vulnerability -	
			Blogs & Documents -	
BMC	MainView	$\operatorname{Under}$	BMC Community BMC Security Advisory	
DMC	Middleware	Investigation	for CVE-2021-44228	
	Monitor		Log4Shell Vulnerability -	
			Blogs & Documents -	
D1.60	D 1 70001		BMC Community	
BMC	Remedy ITSM (IT Service	Under Investigation	BMC Security Advisory for CVE-2021-44228	
	Management)	investigation	Log4Shell Vulnerability -	
	1.20.2080220)		Blogs & Documents -	
			BMC Community	
BMC	SmartIT	Under	BMC Security Advisory	
		Investigation	for CVE-2021-44228 Log4Shell Vulnerability -	
			Blogs & Documents -	
			BMC Community	
BMC	Track-It!	Under	BMC Security Advisory	
		Investigation	for CVE-2021-44228	
			Log4Shell Vulnerability -	
			Blogs & Documents - BMC Community	
BMC	TrueSight	$\operatorname{Under}$	BMC Security Advisory	
	Automation for	Investigation	for CVE-2021-44228	
	Networks	-	Log4Shell Vulnerability -	
			Blogs & Documents -	
			BMC Community	

Matomation for	Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
BMC	BMC								
Binche				Investigation					
March   Marc		Servers				v			
TrueSight									
Capacity   Investigation	DMG	The Civil of		TT 1					
Desiration   Des	BMC								
Back				Investigation					
HMC Community Linder traine Linder traine Linder traine Linder Community L		Optimization							
BMC   Security Advisors									
Forestreet	PMC	TrucSight		Under					
Mainagement	DMC								
BMC				mvcsugamon					
Bill		Management							
BMC									
Pose	BMC	TrueSight		Under					
Minagement									
Binch   Comments   Binch   B				O					
BMC									
Protection   Investigation						BMC Community			
Provided	BMC			Under					
Boson				Investigation		for CVE-2021-44228			
Broto									
Estentific   Under									
Scientific   Sear									
Book									12/20/2021
Box Big Post   Brainworks   Brainworks   BrightSign   Broadcom   Advanced   Under   Broadcom   Broadcom   Advanced   Under   Broadcom   Support									
Brinworks BrightSign         Brainworks Link BrightSign Link           Broadcon Advanced (ASG)         Under         Broadcon Support           Broadcon (ASG)         Westigation         Portal           Broadcon Automation         Automation         Broadcon Automation           Broadcon Automation         Broadcon Support           Broadcon Automation         Broadcon Support           Broadcon Automation         Broadcon Support           Broadcon CA Advanced Automaticon         9.1         Affected           Broadcon CA Risk Authoriteation         Affected         Head Canada Authoriteation           Broadcon CA Strong Authoriteation         Affected         Head Canada Authoriteation           Broadcon Coloul Workload Authoriteation         Under         Broadcon Support           Broadcon Coloul Workload Authoriteation         Under         Broadcon Support           Broadcon Coloul Workload Authoriteation         Under         Broadcon Support           Broadcon Coloul Workload Authoriteation         Under Stores Froiteation Froiteat				Affected	No				12/22/2021
Bright Sign         Broadcom         Bright Sign Link           Broadcom         Advanced Cateway         Investigation         Portal           (ASG)         Automate         Broadcom Automic           Broadcom         Automate         Automate         Broadcom Support           Broadcom         BCAA         Under         Portal           Broadcom         Automated         9.1         Affected           Broadcom         CA Ralvanced         9.1         Affected           Broadcom         CA Ralvanced         Affected         Portal           Broadcom         CA Strong         Affected         Portal           Broadcom         CA Strong         Affected         Broadcom Support           Broadcom         Cloud Workload         Under         Broadcom Support           Broadcom         COWPS)         Portal           Broadcom         Cloud Access         Fortal           Scarge         Fortal         Portal           Broadcom         Condoto         Not Affected         Portal           Broadcom         Condoto         Not Affected         Portal           Broadcom         Content         Under         Portal           Broadcom         Portal									
Bondcom         Advanced         Under         Broadcom Secure Gateway         Investigation         Profata           Broadcom         Automation         — Roadcom Automic         Automation         — Roadcom Support           Broadcom         BCAAA         Under         — Roadcom Support           Broadcom         CA Advanced         9.1         — Affected           Authoriteation         — Authoriteation         — Authoriteation           Broadcom         CA Strong         — Affected           Authoriteation         — Frotestion         — Roadcom Support           Broadcom         COuld Workload         — Under         — Broadcom Support           Broadcom         Cloud Workload         — Under         — Broadcom Support           Broadcom         Cloud Workload         — Under         — Broadcom Support           Broadcom         Cloud Workload         — Under         — Portal           Broadcom         — Could Workload         — Portal         — Portal           Broadcom									
Secur Gateway				TT 1					
ASCG   Astromic   Automation   Inke   Automation   Automation   Inke   Automation   Inke   Automation   Inke   Automation   Inke   Automation   Investigation   Portal	Broadcom								
Broad com				Investigation		Portal			
Automation	D 1	,				Duna lanna Antania			
Broadcom         BCAAA         Under Investigation         Broadcom Support           Broadcom         CA Advanced of Authentication         Affected           Broadcom         CA Risk Authentication         Affected           Broadcom         CA Strong Authentication         Affected           Broadcom         Colvid Workload Color Only Colo	Broadcom								
Droadcom	Drondoom			Undon					
Broadcom         CA Advanced Authentication         9.1         Affected           Broadcom         CA Risk         Affected           Broadcom         CA Strong Authentication         Affected           Broadcom         Cloud Workload Protection (CWP)         Under         Broadcom Support           Broadcom Protection (CWP)         Under         Broadcom Support           Broadcom (CWP)S)         Under         Broadcom Support           Broadcom (CWP)S)         Not Affected         Broadcom Support           Broadcom (CWP)S)         Not Affected         Broadcom Support           Broadcom (Could Workload From the County (CWP)S)         Not Affected         Broadcom Support           Broadcom (CWP)S)         Not Affected         Broadcom Support           Broadcom (County Broker From the County Broadcom Support From the Count	broadcom	DCAAA							
Broadcom         Authentication         Affected           Broadcom         CA Strong         Affected           Broadcom         Cloud Workload         Under         Broadcom Support           Broadcom         Protection         Investigation         Portal           Broadcom         Cloud Workload         Under         Broadcom Support           Broadcom         Cloud Workload         Under         Broadcom Support           Protection for         Investigation         Portal           Korage         CWP'S)         Very Signature           Broadcom         Cloud Access         Portal           Security Broker         CASB)         Portal           Broadcom         Content         Under         Broadcom Support           Broadcom         Contical System         Investigation         Portal           Broadcom         Citical System         Investigation         Portal           Broadcom         Data Loss         Not Affected         Broadcom Support           Broadcom         Janabase Center         Not Affected         Broadcom Support           Broadcom         Janabase Center         Not Affected         Broadcom Support           Broadcom         Data Loss         Not Affected	Brondoom	CA Advanced	0.1			Fortar			
Broadcom Authentication         CA Strong Authentication         Authentication           Broadcom Cond Workload Protection (CWP)         Under Protection (CWP)         Broadcom Support           Broadcom Protection (CWP)         Under Protection (CWP)         Broadcom Support           Broadcom Protection (CWP)         Under Protection (CWP)         Broadcom Support           Broadcom (CWPS)         Worklead (CWPS)         Broadcom Support           Broadcom (CWPS)         Worklead (CWPS)         Broadcom Support           Broadcom (CWPS)         Portal         Broadcom Support           Broadcom (Could Access (CWPS)         Fortal         Broadcom Support           Broadcom (Costes)         Fortal         Broadcom Support           Broadcom (Costes)         Investigation (CSP)         Portal           Broadcom (Costes)         Investigation (CSP)         Portal           Broadcom (CSP)         Broadcom Support (CSP)           Broadcom (CSP)         Broadcom (CSP)           Broadcom (CSP)	Dioadcom		9.1	Allected					
$ \begin{tabular}{l l l l l l l l l l l l l l l l l l l $	Broadcom			Affected					
Broadcom Cloud Workload Under Broadcom Support    Cloud Workload Under Broadcom Support	Broadcom			Hilococa					
$ \text{Broadcom} \\ \text{Broadcom} \\ \text{Cloud Workload} \\ \text{Protection} \\ \text{CWP} \\ \text{Broadcom} \\ \text{Cloud Workload} \\ \text{Protection} \\ \text{Cloud Workload} \\ \text{Protection for} \\ \text{Storage} \\ \text{CWP/S} \\ \text{CWP/S} \\ \text{Broadcom} \\ \text{Cloud SOC} \\ \text{CWP/S} \\ \text{Broadcom} \\ \text{Portection for} \\ \text{Storage} \\ \text{CWP/S} \\ \text{CWP/S} \\ \text{CWP/S} \\ \text{Broadcom} \\ \text{Portal} \\ \text{Endodeom} \\ \text{Portal} \\ \text{Cold SOC} \\ \text{Scurity Broker} \\ \text{CASB} \\ \text{Foreign for the stigation} \\ \text{Portal} \\ $	Broadcom			Affected					
Broadcom Cloud Workload Investigation Investigation Portal (CWP)  Broadcom Cloud Workload Investigation Investigat									
Protection (CWP)  Broadcom Cloud Workload Under Broadcom Support  Protection for Investigation Portal  Storage (CWP:S)  Broadcom Cloud SOC Not Affected Portal  Security Broker (CASB)  Broadcom Content Analysis (CA) Investigation Portal  Broadcom Portal  Froadcom Couting System Under Broadcom Support  Analysis (CA) Investigation Portal  Broadcom Portal  Broadcom Portal  Broadcom Support  Analysis (CA) Investigation Portal  CSP)  Broadcom Support  Portal  Broadcom Support  Portal  Broadcom Support  Portal  Froadcom Support  Fr	Broadcom			Under		Broadcom Support			
Protection for Storage (CWP-S)  Broadcom Cloud Access (CASB)  Broadcom Content (CASB)  Broadcom Content (CSP)  Broadcom Support (CSP)									
Storage (CWP:S)  Broadcom Cloud SOC Not Affected Broadcom Support Cloud Access Security Broker (CASB)  Broadcom Content Analysis (CA) Investigation Protection Protection Protection Protection COSP)  Broadcom Broadcom Broadcom Data Center Security DCS)  Broadcom Data Loss Prevention Prevention Data Loss Prevention Data Loss Prevention Data Loss Prevention Data Center Security DCS) Broadcom Broadcom Data Loss Prevention Data Loss Data	Broadcom			$\operatorname{Under}$		Broadcom Support			
$ \begin{array}{c} (CWP:S) \\ Foadcom $		Protection for		Investigation					
Broadcom Cloud SOC Not Affected Broadcom Support Cloud Access Portal  Security Broker (CASB)  Broadcom Content Under Broadcom Support Portal  Broadcom Critical System Under Broadcom Support Protection (CSP)  Broadcom Potat Cester Not Affected Broadcom Support Portal  Broadcom Broadcom Support Protection (CSP)  Broadcom Data Center Not Affected Broadcom Support Portal  Broadcom Data Loss Not Affected Broadcom Support Portal  Broadcom Data Loss Not Affected Broadcom Support Prevention Portal  Broadcom Data Loss Not Affected Broadcom Support Prevention Portal  Broadcom Broadcom Support Prevention Portal  Broadcom Support Broadcom Support Prevention Support Prevention Portal  Broadcom Support Prevention Support Prevention Portal  Broadcom Support Prevention Support Prevention Portal  Broadcom Support Prevention Portal  Broadcom Support Portal		Storage							
Cloud Access   Security Broker   Security Broker   CASB   Security Broker   Content   Under   Broadcom Support   Security Broadcom   Data Center   Data Center   Security (DCS)   Data Coss   Security (DCS)   Sec									
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	Broadcom			Not Affected					
CASB   Content   Under   Broadcom Support						Portal			
Broadcom Content Under Broadcom Support Analysis (CA) Investigation Portal Broadcom Critical System Under Broadcom Support Protection Investigation Portal (CSP) Broadcom Data Center Not Affected Portal Broadcom Data Loss Prevention Portal Broadcom Data Loss Prevention Data Loss Broadcom Support Prevention Broadcom Support									
Analysis (CA) Broadcom Critical System Under Broadcom Portal Broadcom Support Protection (CSP) Broadcom Data Center Security (DCS) Broadcom Data Loss Prevention Portal Broadcom Data Loss Portal Broadcom Data Loss Prevention Data Loss Prevention Data Loss Prevention Data Loss Prevention Data Loss Broadcom Support Prevention Data Loss Broadcom Support Broadcom Support Portal Broadcom Support Broadcom Support Portal Broadcom Support									
Broadcom Critical System Under Broadcom Support Protection Investigation Portal (CSP)  Broadcom Data Center Not Affected Broadcom Support Security (DCS)  Broadcom Data Loss Not Affected Broadcom Support Prevention Portal (DLP)  Broadcom Email Security Under Broadcom Support Protal	Broadcom								
Protection (CSP)  Broadcom Data Center Not Affected Portal  Broadcom Data Loss Not Affected Portal  Broadcom Support  Portal  Portal  Broadcom Support  Portal  Broadcom Support  Portal  DLP)									
Broadcom   Data Center   Not Affected   Broadcom Support     Security (DCS)   Portal     Broadcom   Data Loss   Not Affected   Broadcom Support     Prevention   Portal     (DLP)     Broadcom   Email Security   Under   Broadcom Support	Broadcom								
Broadcom Data Center Not Affected Broadcom Support Portal  Broadcom Data Loss Not Affected Broadcom Support Portal  Broadcom Data Loss Prevention Portal Prevention (DLP)  Broadcom Email Security Under Broadcom Support Broadcom Support Product Pro				Investigation		Portal			
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	D 1			37 / 100 -		D 1 0			
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	Broadcom			Not Affected					
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	ъ.			** . 1 m · -					
(DLP) Broadcom Email Security Under Broadcom Support	Broadcom			Not Affected					
Broadcom Email Security Under Broadcom Support						Portal			
	D 1			77 1		D 1 0			
Service (ESS) Investigation Portal	Broadcom								
		Service (ESS)		Investigation		Portal			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Broadcom	Ghost Solution Suite (GSS)		Not Affected		Broadcom Support Portal			
Broadcom	HSM Agent		Under		Broadcom Support			
Broadcom	Industrial		Investigation Under		Portal Broadcom Support			
Dioagcom	Control System		Investigation		Portal			
	Protection		11110001901011		1 02 002			
Broadcom	(ICSP) Integrated		Under		Broadcom Support			
Dioadcom	Cyber Defense		Investigation		Portal			
	Manager		investigation		1 01000			
	(ICDm)							
Broadcom	Integrated		Under		Broadcom Support			
	Secure Gateway		Investigation		Portal			
Broadcom	(ISG) IT Management		Not Affected		Broadcom Support			
Dioadcom	Suite		Not Affected		Portal			
Broadcom	Layer7 API		Under		Broadcom Support			
	Developer		Investigation		Portal			
	Portal							
Broadcom	Layer7 API Gateway		Not Affected		Broadcom Support Portal			
Broadcom	Layer7 Mobile		Not Affected		Broadcom Support			
Dioadcom	API Gateway		1100 Milected		Portal			
Broadcom	Management		Under		Broadcom Support			
	Center (MC)		Investigation		Portal			
Broadcom	PacketShaper		Under		Broadcom Support			
Broadcom	(PS) S-Series PolicyCenter		Investigation Under		Portal Broadcom Support			
Broadcom	(PC) S-Series		Investigation		Portal			
Broadcom	Privileged		Under		Broadcom Support			
	Access Manager		Investigation		Portal			
Broadcom	Privileged		Under		Broadcom Support			
	Access Manager Server Control		Investigation		Portal			
Broadcom	Privileged		Under		Broadcom Support			
	Identity		Investigation		Portal			
D 1	Manager		N A.C 1		D 1 C .			
Broadcom	ProxySG		Not Affected		Broadcom Support Portal			
Broadcom	Reporter		Under		Broadcom Support			
			Investigation		Portal			
$\operatorname{Broadcom}$	Secure Access		Under		Broadcom Support			
D 1	Cloud (SAC)		Investigation		Portal			
Broadcom	Security Analytics (SA)		Not Affected		Broadcom Support Portal			
Broadcom	SiteMinder (CA		Under		Broadcom Support			
Diodacom	Single Sign-On)		Investigation		Portal			
${\bf Broadcom}$	SSL Visibility		Under		Broadcom Support			
D 1	(SSLV)		Investigation		Portal			
Broadcom	Symantec Control		Not Affected		Broadcom Support Portal			
	Compliance				Fortai			
	Suite (CCS)							
$\operatorname{Broadcom}$	Symantec		Not Affected		Broadcom Support			
<b>.</b> .	Directory				Portal			
Broadcom	Symantec		Under		Broadcom Support			
	Endpoint Detection and		Investigation		Portal			
	Response							
	(EDR)							
$\operatorname{Broadcom}$	Symantec		Under		Broadcom Support			
	Endpoint		Investigation		Portal			
	Encryption (SEE)							
	(SEEE)							

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Broadcom	Symantec		Under		Broadcom Support			
	Endpoint		Investigation		Portal			
	Protection (SEP)							
Broadcom	Symantec		Under		Broadcom Support			
	Endpoint		Investigation		Portal			
	Protection (SEP) for							
	Mobile							
Broadcom	Symantec	14.3	Affected	No	Broadcom Support			
	Endpoint Protection				Portal			
	Manager							
D 1	(SEPM)		N A C A		D 1 0			
Broadcom	Symantec Identity		Not Affected		Broadcom Support Portal			
	Governance and				1 01 001			
	Administration							
Broadcom	(IGA) Symantec Mail		Under		Broadcom Support			
Broadcom	Security for		Investigation		Portal			
	Microsoft							
	Exchange (SMSMSE)							
Broadcom	Symantec		Under		Broadcom Support			
	Messaging		Investigation		Portal			
Broadcom	Gateway (SMG) Symantec PGP		Not Affected		Broadcom Support			
	Solutions				Portal			
Broadcom	Symantec Protection		Under		Broadcom Support			
	Engine (SPE)		Investigation		Portal			
Broadcom	Symantec		Under		Broadcom Support			
	Protection for SharePoint		Investigation		Portal			
	Servers (SPSS)							
Broadcom	VIP		Not Affected		Broadcom Support			
Broadcom	VIP		Under		Portal Broadcom Support			
	Authentication		Investigation		Portal			
Duos do ous	Hub Web Isolation		Under		Broadcom Support			
Broadcom	(WI)		Investigation		Portal			
Broadcom	Web Security		Under		Broadcom Support			
Broadcom	Service (WSS) WebPulse		Investigation Under		Portal Broadcom Support			
Broadcom	Webi uise		Investigation		Portal			
C4b					C4b XPHONE Link			
XPHONE Campbell	All		Not Affected		Campbell Scientific			12/23/2021
Scientific			1.00 111100000		Statement			1-/ -0/ -0-1
Camunda	A 11		N-+ AG+-1		Camunda Forum Link			10/00/0001
Canary Labs	All		Not Affected		Canary Labs Advisory Link			12/22/2021
Canon	CT Medical		Not Affected		Canon Advisory Link			12/22/2021
	Imaging Products							
Canon	MR Medical		Not Affected		Canon Advisory Link			12/22/2021
	Imaging				v			, ,
Canon	Products UL Medical		Not Affected		Canon Advisory Link			12/22/2021
Canon	Imaging		Not Affected		Canon Advisory Link			12/22/2021
~	Products							10 /00 /055
Canon	XR Medical Imaging		Not Affected		Canon Advisory Link			12/22/2021
	Products							

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Canon	NM Medical	.,	Not Affected		Canon Advisory Link			12/22/2021
	Imaging							
Canon	Products Vitrea		Under		Canon Advisory Link			12/22/2021
Canon	Advanced 7.x		Investigation					12/22/2021
Canon	Infinix-i (Angio		Under		Canon Advisory Link			12/22/2021
Canon	Workstation) Alphenix (Angio		Investigation Under		Canon Advisory Link			12/22/2021
	Workstation)		Investigation		·			
CapStorm	Copystorm		Under Investigation					12/22/2021
CarbonBlack					CarbonBlack Advisory			
Carestream			Not Affected		Carestream Advisory Link			12/20/2021
CAS					CAS genesisWorld Link			
genesisWorld					C + N + 1 D			
Cato Networks					Cato Networks Blog Post			
Cepheid	C360		Not Affected		Cepheid Advisory Link			12/20/2021
Cepheid	GeneXpert		Under Investigation		Cepheid Advisory Link			12/20/2021
Cerberus			Investigation		Cerberus Article			
FTP	1: · · · · NI A/T	A 11	N. A.C. 4 1		A Cl 1 1 1			
Chaser Systems	discrimiNAT Firewall	All	Not Affected		Are Chaser's products affected			
Check Point	CloudGuard	All	Not Affected		sk176865			
Check Point	Harmony Endpoint &	All	Not Affected		sk176865			
	Harmony							
Cl. l.D.:	Mobile		N. A.C. 4 1		1170005			
Check Point Check Point	Infinity Portal Quantum	All	Not Affected Not Affected		sk176865 sk176865			
	Security							
Check Point	Gateway Quantum	All	Not Affected		sk176865	Where		
	Security		1100 111100004		511,0000	used, uses		
	Management					the 1.8.0_u241		
						version of		
						the JRE		
						that protects		
						against		
						this attack by default.		
Check Point	SMB	All	Not Affected		sk176865	by deladio.		
Check Point	ThreatCloud		Not Affected		sk176865 CheckMK Forum			
CheckMK Ciphermail					Ciphermail Blog Post			
CIS			A. (7)	**	CIS Customer Portal			
Cisco	AppDynamics		Affected	Yes	Vulnerability in Apache Log4j Library Affecting			
					Cisco Products:			
Cisco	Cisco Common		Under		December 2021 Vulnerability in Apache			
0.1500	Services		Investigation		Log4j Library Affecting			
	Platform Collector				Cisco Products: December 2021			
Cisco	Collector Cisco Network		Affected	No	Vulnerability in Apache			
	Services				Log4j Library Affecting			
	Orchestrator (NSO)				Cisco Products: December 2021			
Cisco	Cisco System		Under		Vulnerability in Apache			
			Investigation					
	Gateway				December 2021			
	(SAEGW)							
Cisco	Architecture Evolution Gateway				Log4j Library Affecting Cisco Products:			

Vendor	Product	Version(s) Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cisco	Cisco ACI	Under		Vulnerability in Apache			
	Multi-Site	Investigation	1	Log4j Library Affecting			
	Orchestrator			Cisco Products:			
C:	C: ACI	TT 1		December 2021			
Cisco	Cisco ACI	Under		Vulnerability in Apache			
	Virtual Edge	Investigation	1	Log4j Library Affecting Cisco Products:			
				December 2021			
Cisco	Cisco Adaptive	Under		Vulnerability in Apache			
	Security	Investigation	1	Log4j Library Affecting			
	Appliance			Cisco Products:			
	(ASA) Software			December 2021			
Cisco	Cisco Advanced	Affected	No	Vulnerability in Apache			
	Web Security			Log4j Library Affecting			
	Reporting			Cisco Products:			
C:	Application	TT 1		December 2021			
Cisco	Cisco AMP Virtual Private	Under		Vulnerability in Apache			
	Cloud	Investigation	1	Log4j Library Affecting Cisco Products:			
	Appliance			December 2021			
Cisco	Cisco	Under		Vulnerability in Apache			
CIBCO	AnyConnect	Investigation		Log4j Library Affecting			
	Secure Mobility			Cisco Products:			
	Client			December 2021			
Cisco	Cisco	$\operatorname{Under}$		Vulnerability in Apache			
	Application	Investigation	1	Log4j Library Affecting			
	Policy			Cisco Products:			
	Infrastructure			December 2021			
	Controller						
Cisco	(APIC) Cisco ASR 5000	Under		Vulnerability in Apache			
Cisco	Series Routers	Investigation		Log4j Library Affecting			
	Series reducers	investigatio.	•	Cisco Products:			
				December 2021			
Cisco	Cisco	Under		Vulnerability in Apache			
	Broadcloud	Investigation	1	Log4j Library Affecting			
	Calling			Cisco Products:			
				December 2021			
Cisco	Cisco	Under		Vulnerability in Apache			
	BroadWorks	Investigation	1	Log4j Library Affecting			
				Cisco Products: December 2021			
Cisco	Cisco Catalyst	Under		Vulnerability in Apache			
Cisco	9800 Series	Investigation	1	Log4j Library Affecting			
	Wireless	invostigatio.	•	Cisco Products:			
	Controllers			December 2021			
Cisco	Cisco	Affected	No	Vulnerability in Apache			
	CloudCenter			Log4j Library Affecting			
	Suite Admin			Cisco Products:			
	C.			December 2021			
Cisco	Cisco	Under		Vulnerability in Apache			
	CloudCenter	Investigation	1	Log4j Library Affecting			
	Workload Manager			Cisco Products: December 2021			
Cisco	Cisco Cognitive	Under		Vulnerability in Apache			
C1500	Intelligence	Investigation	1	Log4j Library Affecting			
		iiivoongano.	-	Cisco Products:			
				December 2021			
Cisco	Cisco Computer	Affected	No	Vulnerability in Apache			
	Telephony			Log4j Library Affecting			
	Integration			Cisco Products:			
	Object Server			December 2021			
G:	(CTIOS)			37.1 1.11			
Cisco	Cisco	Under	_	Vulnerability in Apache			
	Connected Grid Device Manager	Investigation	1	Log4j Library Affecting Cisco Products:			
	Device manager			December 2021			
				December 2021			

Vendor	Product	Version(s) Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cisco	Cisco	Under		Vulnerability in Apache			
	Connected	Investigati	on	Log4j Library Affecting			
	Mobile			Cisco Products:			
	Experiences			December 2021			
Cisco	Cisco	Under		Vulnerability in Apache			
	Connectivity	Investigati	on	Log4j Library Affecting			
				Cisco Products:			
				December 2021			
Cisco	Cisco Contact	Under		Vulnerability in Apache			
	Center Domain	Investigati	on	Log4j Library Affecting			
	Manager			Cisco Products:			
~.	(CCDM)			December 2021			
Cisco	Cisco Contact	Under		Vulnerability in Apache			
	Center	Investigati	on	Log4j Library Affecting			
	Management			Cisco Products:			
CI:	Portal (CCMP)	A.C 1	N	December 2021			
Cisco	Cisco Crosswork	Affected	No	Vulnerability in Apache			
	Change			Log4j Library Affecting			
	Automation			Cisco Products: December 2021			
Ciasa	Cisco CX Cloud	II. don					
Cisco	Agent Software	Under Investigati	on.	Vulnerability in Apache Log4j Library Affecting			
	Agent Software	mvestigati	OII	Cisco Products:			
				December 2021			
Cisco	Cisco Data	Under		Vulnerability in Apache			
Cisco	Center Network	Investigati	on	Log4j Library Affecting			
	Manager	mvestigati	<i>J</i> 11	Cisco Products:			
	(DCNM)			December 2021			
Cisco	Cisco Defense	Under		Vulnerability in Apache			
Cisco	Orchestrator	Investigati	on	Log4j Library Affecting			
	Orchestrator	1111/05018401	<i>,</i> 11	Cisco Products:			
				December 2021			
Cisco	Cisco DNA	Under		Vulnerability in Apache			
	Assurance	Investigati	on	Log4j Library Affecting			
				Cisco Products:			
				December 2021			
Cisco	Cisco DNA	Under		Vulnerability in Apache			
	Center	Investigati	on	Log4j Library Affecting			
				Cisco Products:			
				December 2021			
Cisco	Cisco DNA	Under		Vulnerability in Apache			
	Spaces	Investigati	on	Log4j Library Affecting			
				Cisco Products:			
				December 2021			
Cisco	DUO network	Under					
	gateway	Investigati	on				
	(on-prem/self-						
C:	hosted)	TT 1		17.1 1.2124 · A 1			
Cisco	Cisco Elastic	Under		Vulnerability in Apache			
	Services Controller	Investigati	ш	Log4j Library Affecting Cisco Products:			
	(ESC)			December 2021			
Cisco	(ESC) Cisco	$\operatorname{Under}$		Vulnerability in Apache			
Cisco	Emergency	Investigati	on	Log4j Library Affecting			
	Responder	investigati	, <u>,,,</u>	Cisco Products:			
	responder			December 2021			
Cisco	Cisco Enterprise	Under		Vulnerability in Apache			
	Chat and Email	Investigati	on	Log4j Library Affecting			
	Char and Lindii	investigati		Cisco Products:			
				December 2021			
Cisco	Cisco Enterprise	Under		Vulnerability in Apache			
-2200	NFV	Investigati	on	Log4j Library Affecting			
	Infrastructure	111100016001		Cisco Products:			
	Software			December 2021			
	(NFVIS)						
	. =/						

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last	Updated
Cisco	Cisco Evolved Programmable		Affected	No	Vulnerability in Apache Log4j Library Affecting				
	Network				Cisco Products:				
a.	Manager		** 1		December 2021				
Cisco	Cisco Extensible		Under		Vulnerability in Apache				
	Network Controller		Investigation		Log4j Library Affecting Cisco Products:				
	(XNC)				December 2021				
Cisco	Cisco Finesse		Under		Vulnerability in Apache				
Cisco	Cisco i messe		Investigation		Log4j Library Affecting				
			11110001801011		Cisco Products:				
					December 2021				
Cisco	Cisco Firepower		Under		Vulnerability in Apache				
	Management		Investigation		Log4j Library Affecting				
	Center				Cisco Products:				
					December 2021				
Cisco	Cisco Firepower		Under		Vulnerability in Apache				
	Threat Defense		Investigation		Log4j Library Affecting				
	(FTD)				Cisco Products: December 2021				
Cisco	Cisco GGSN		Under		Vulnerability in Apache				
Cisco	Gateway GPRS		Investigation		Log4j Library Affecting				
	Support Node		investigation		Cisco Products:				
	Support 1.ode				December 2021				
Cisco	Cisco HyperFlex		Under		Vulnerability in Apache				
	System		Investigation		Log4j Library Affecting				
					Cisco Products:				
					December 2021				
Cisco	Cisco Identity		Under		Vulnerability in Apache				
	Services Engine		Investigation		Log4j Library Affecting				
	(ISE)				Cisco Products:				
Cisco	Ciasa Intermeted		Affected	No	December 2021 Vulnerability in Apache				
Cisco	Cisco Integrated Management		Affected	NO	Log4j Library Affecting				
	Controller				Cisco Products:				
	(IMC)				December 2021				
	Supervisor				2000				
Cisco	Cisco Intersight		Under		Vulnerability in Apache				
			Investigation		Log4j Library Affecting				
					Cisco Products:				
					December 2021				
Cisco	Cisco Intersight		Affected	No	Vulnerability in Apache				
	Virtual				Log4j Library Affecting				
	Appliance				Cisco Products: December 2021				
Cisco	Cisco IOS and		Under		Vulnerability in Apache				
Cisco	IOS XE		Investigation		Log4j Library Affecting				
	Software		investigation		Cisco Products:				
	20111101				December 2021				
Cisco	Cisco IoT Field		Under		Vulnerability in Apache				
	Network		Investigation		Log4j Library Affecting				
	Director				Cisco Products:				
	(formerly Cisco				December 2021				
	Connected Grid								
	Network								
	Management								
Cisco	System) Cisco IoT		Under		Vulnerability in Apache				
Cisco	Operations		Investigation		Log4j Library Affecting				
	Dashboard		mvesugation		Cisco Products:				
	Daniboard				December 2021				
Cisco	Cisco IOx Fog		Under		Vulnerability in Apache				
	_				Log4j Library Affecting				
	Director		investigation		Log4 Library Anecung				
	Director		Investigation		Cisco Products:				

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cisco	Cisco IP		Under		Vulnerability in Apache			
	Services		Investigation		Log4j Library Affecting			
	Gateway				Cisco Products:			
	(IPSG)				December 2021			
Cisco	Cisco Kinetic		Affected	No	Vulnerability in Apache			
	for Cities				Log4j Library Affecting			
					Cisco Products:			
Cisco	Cisco MDS 9000		Under		December 2021 Vulnerability in Apache			
Cisco	Series		Investigation		Log4j Library Affecting			
	Multilayer		investigation		Cisco Products:			
	Switches				December 2021			
Cisco	Cisco Meeting		Under		Vulnerability in Apache			
	Server		Investigation		Log4j Library Affecting			
					Cisco Products:			
					December 2021			
Cisco	Cisco MME		Under		Vulnerability in Apache			
	Mobility		Investigation		Log4j Library Affecting			
	Management Entity				Cisco Products: December 2021			
Cisco	Cisco Modeling		Under		Vulnerability in Apache			
Cisco	Labs		Investigation		Log4j Library Affecting			
			222.000.8000		Cisco Products:			
					December 2021			
Cisco	Cisco Network		Under		Vulnerability in Apache			
	Assessment		Investigation		Log4j Library Affecting			
	(CNA) Tool				Cisco Products:			
C:	C: N. I		TT 1		December 2021			
Cisco	Cisco Network Assurance		Under Investigation		Vulnerability in Apache Log4j Library Affecting			
	Engine Engine		Investigation		Cisco Products:			
	Liigine				December 2021			
Cisco	Cisco Network		Under		Vulnerability in Apache			
	Convergence		Investigation		Log4j Library Affecting			
	System 2000				Cisco Products:			
	Series				December 2021			
Cisco	Cisco Network		Under		Vulnerability in Apache			
	Planner		Investigation		Log4j Library Affecting Cisco Products:			
					December 2021			
Cisco	Cisco Nexus		Under		Vulnerability in Apache			
	5500 Platform		Investigation		Log4j Library Affecting			
	Switches				Cisco Products:			
					December 2021			
Cisco	Cisco Nexus		Under		Vulnerability in Apache			
	5600 Platform		Investigation		Log4j Library Affecting			
	Switches				Cisco Products: December 2021			
Cisco	Cisco Nexus		Under		Vulnerability in Apache			
CISCO	6000 Series		Investigation		Log4j Library Affecting			
	Switches		O		Cisco Products:			
					December 2021			
Cisco	Cisco Nexus		Under		Vulnerability in Apache			
	7000 Series		Investigation		Log4j Library Affecting			
	Switches				Cisco Products:			
Cisco	Cisco Nexus		Under		December 2021			
Cisco	9000 Series		Investigation		Vulnerability in Apache Log4j Library Affecting			
	Fabric Switches		mvcsugation		Cisco Products:			
	in Application				December 2021			
	Centric				-			
	Infrastructure							
	(ACI) mode							
Cisco	Cisco Nexus		Under		Vulnerability in Apache			
	Dashboard		Investigation		Log4j Library Affecting			
	(formerly Cisco Application				Cisco Products: December 2021			
	Services Engine)				December 2021			
	sorvices Engine)							

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cisco	Cisco Nexus		Under		Vulnerability in Apache			
	Data Broker		Investigation		Log4j Library Affecting			
					Cisco Products:			
G:	CI N		TT 1		December 2021			
Cisco	Cisco Nexus		Under		Vulnerability in Apache			
	Insights		Investigation		Log4j Library Affecting Cisco Products:			
					December 2021			
Cisco	Cisco Optical		Under		Vulnerability in Apache			
	Network		Investigation		Log4j Library Affecting			
	Planner				Cisco Products:			
G:	C: D 1 1		A.C 1	N	December 2021			
Cisco	Cisco Packaged Contact Center		Affected	No	Vulnerability in Apache Log4j Library Affecting			
	Enterprise				Cisco Products:			
	zmerprise				December 2021			
Cisco	Cisco Paging		Under		Vulnerability in Apache			
	Server		Investigation		Log4j Library Affecting			
	(InformaCast)				Cisco Products:			
C:	C: D :		TT 1		December 2021			
Cisco	Cisco Paging Server		Under Investigation		Vulnerability in Apache Log4j Library Affecting			
	Server		Investigation		Cisco Products:			
					December 2021			
Cisco	Cisco		Under		Vulnerability in Apache			
	PDSN/HA		Investigation		Log4j Library Affecting			
	Packet Data				Cis co Products:			
	Serving Node				December 2021			
	$egin{array}{c}  ext{and Home} \  ext{Agent} \end{array}$							
Cisco	Cisco PGW		Under		Vulnerability in Apache			
01000	Packet Data		Investigation		Log4j Library Affecting			
	Network				Cisco Products:			
	Gateway				December 2021			
Cisco	Cisco Policy		Under		Vulnerability in Apache			
	Suite		Investigation		Log4j Library Affecting Cisco Products:			
					December 2021			
Cisco	Cisco Prime		Under		Vulnerability in Apache			
	Central for		Investigation		Log4j Library Affecting			
	Service				Cisco Products:			
G:	Providers		TT 1		December 2021			
Cisco	Cisco Prime Collaboration		Under Investigation		Vulnerability in Apache Log4j Library Affecting			
	Manager		Investigation		Cisco Products:			
	11101101501				December 2021			
Cisco	Cisco Prime		Under		Vulnerability in Apache			
	Collaboration		Investigation		Log4j Library Affecting			
	Provisioning				Cisco Products: December 2021			
Cisco	Cisco Prime		Under		Vulnerability in Apache			
Cisco	Infrastructure		Investigation		Log4j Library Affecting			
					Cisco Products:			
					December 2021			
Cisco	Cisco Prime		Under		Vulnerability in Apache			
	License		Investigation		Log4j Library Affecting			
	Manager				Cisco Products: December 2021			
Cisco	Cisco Prime		Under		Vulnerability in Apache			
02.00	Network		Investigation		Log4j Library Affecting			
			0		Cisco Products:			
					December 2021			
Cisco	Cisco Prime		Under		Vulnerability in Apache			
	Optical for		Investigation		Log4j Library Affecting			
	Service Providers				Cisco Products: December 2021			
	1 TOVIGETS				DOGUMUCI 2021			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cisco	Cisco Prime		Under		Vulnerability in Apache			
	Provisioning		Investigation		Log4j Library Affecting			
	-				Cisco Products:			
	Gt :				December 2021			
Cisco	Cisco Prime		Under		Vulnerability in Apache			
	Service Catalog		Investigation		Log4j Library Affecting Cisco Products:			
					December 2021			
Cisco	Cisco Registered		Under		Vulnerability in Apache			
	Envelope		Investigation		Log4j Library Affecting			
	Service				Cisco Products:			
					December 2021			
Cisco	Cisco SD-WAN		Under		Vulnerability in Apache			
	vEdge 1000		Investigation		Log4j Library Affecting Cisco Products:			
	Series Routers				December 2021			
Cisco	Cisco SD-WAN		Under		Vulnerability in Apache			
CIBCO	vEdge 2000		Investigation		Log4j Library Affecting			
	Series Routers		g		Cisco Products:			
					December 2021			
Cisco	Cisco SD-WAN		Under		Vulnerability in Apache			
	vEdge 5000		Investigation		Log4j Library Affecting			
	Series Routers				Cisco Products: December 2021			
Cisco	Cisco SD-WAN		Under		Vulnerability in Apache			
Cisco	vEdge Cloud		Investigation		Log4j Library Affecting			
	Router Platform		investigation		Cisco Products:			
					December 2021			
Cisco	Cisco SD-WAN		Under		Vulnerability in Apache			
	vManage		Investigation		Log4j Library Affecting			
					Cisco Products:			
Cisco	Cisco Secure		Under		December 2021 Vulnerability in Apache			
Cisco	Network		Investigation		Log4j Library Affecting			
	Analytics		Investigation		Cisco Products:			
	(SNA), formerly				December 2021			
	Stealthwatch							
Cisco	Cisco		Under		Vulnerability in Apache			
	SocialMiner		Investigation		Log4j Library Affecting			
					Cisco Products: December 2021			
Cisco	Cisco		Under		Vulnerability in Apache			
	TelePresence		Investigation		Log4j Library Affecting			
	Management		0		Cisco Products:			
	Suite				December 2021			
Cisco	Cisco UCS		Affected	No	Vulnerability in Apache			
	Director				Log4j Library Affecting Cisco Products:			
					December 2021			
Cisco	Cisco UCS		Under		Vulnerability in Apache			
	Performance		Investigation		Log4j Library Affecting			
	Manager		_		Cisco Products:			
					December 2021			
Cisco	Cisco Umbrella		Affected	No	Vulnerability in Apache			
					Log4j Library Affecting Cisco Products:			
					December 2021			
Cisco	Cisco Unified		Under		Vulnerability in Apache			
<u></u>	Attendant		Investigation		Log4j Library Affecting			
	Console		3		Cisco Products:			
	Advanced				December 2021			
Cisco	Cisco Unified		Under		Vulnerability in Apache			
	Attendant		Investigation		Log4j Library Affecting			
	Console Business				Cisco Products: December 2021			
	Edition Edition				December 2021			
	Lamoun							

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Citrix	Citrix ADC	All Platforms	Not Affected		Citrix Statement	Citrix		12/21/2021
	(NetScaler					continues		
	ADC) and					to		
	Citrix Gateway					investigate		
	(NetScaler					any		
	Gateway)					potential		
						impact on		
						Citrix-		
						managed		
						cloud		
						services.		
						If, as the		
						investiga-		
						tion		
						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.		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Vendor Citrix	Product  Citrix Application Delivery Management (NetScaler MAS)	Version(s) All Platforms	Status Not Affected	Update Available	Vendor Link Citrix Statement	Citrix continues to investigate any potential impact on Citrix- managed cloud services. If, as the investiga- tion 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	Last Updated 12/21/2021
						cloud services do	
						services do not need to take any action.	

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
itrix	Citrix Cloud		Not Affected		Citrix Statement	Citrix		12/21/2021
	Connector					continues		
						to		
						investigate		
						any		
						potential		
						impact on		
						Citrix-		
						managed		
						cloud		
						services.		
						If, as the		
						investiga-		
						tion		
						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.		

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Citrix	Citrix Content		Not Affected		Citrix Statement	Citrix		12/21/2021
	Collaboration					continues		
	(ShareFile					to		
	${\rm Integration}) -\\$					investigate		
	Citrix Files for					any		
	Windows, Citrix					potential		
	Files for Mac,					impact on		
	Citrix Files for					Citrix-		
	Outlook					managed		
						cloud		
						services.		
						If, as the		
						investiga-		
						tion		
						continues,		
						any Citrix-	-	
						managed		
						services		
						are found		
						to be		
						affected by	7	
						this issue,		
						Citrix will		
						take		
						immediate		
						action to		
						remediate		
						the		
						problem.		
						Customers		
						using		
						Citrix-		
						managed		
						cloud		
						services do	•	
						not need		
						to take		
						any action.		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Citrix	Citrix Endpoint		Affected	Yes	Citrix Statement	For		12/21/2021
	Management					CVE-2021-		
	(Citrix					44228 and		
	XenMobile					CVE-2021-		
	Server)					45046:		
						Impacted-		
						Customers		
						are		
						advised to		
						apply the		
						$_{ m CEM}$		
						rolling		
						patch		
						updates		
						listed		
						below as		
						soon as		
						possible to		
						reduce the		
						risk of ex-		
						ploitation.		
						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 recom-		
						mended		
						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:		
						Investiga-		
					42	tion in		
					12	progress.		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Citrix	Citrix		Not Affected		Citrix Statement	Citrix		12/21/2021
	Hypervisor					continues		
	(XenServer)					to		
						investigate		
						any		
						potential		
						impact on		
						Citrix-		
						managed		
						cloud		
						services.		
						If, as the		
						investiga-		
						tion		
						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.		

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
itrix	ShareFile		Not Affected		Citrix Statement	Citrix		12/21/2021
	Storage Zones					continues		
	Controller					to		
						investigate		
						any		
						potential		
						impact on		
						Citrix-		
						managed		
						cloud		
						services.		
						If, as the		
						investiga-		
						tion		
						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.		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Vendor Citrix	Product  Citrix Virtual Apps and Desktops (XenApp & XenDesktop)	Version(s)	Status Affected	Update Available	Vendor Link Citrix Statement	IMPACTEI Linux VDA (non- LTSR versions only)- CVE-2021- 44228 and	D:	Last Updated 12/21/2021
						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 IM- PACTED: Linux VDA LTSR all versions; All other CVAD components		

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

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

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

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cohesity CommVault					Cohesity Support Link CommVault			
Concourse	Concourse		Not affected		Documentation Concourse Community Discussion			
ConcreteCMS. Confluent	.com Confluent Cloud	N/A	Fixed		ConcreteCMS.com Link December 2021 Log4j			12/17/2021
Confluent	Confluent Platform	<7.0.1	Affected	Yes	Vulnerabilities Advisory December 2021 Log4j Vulnerabilities Advisory			12/17/2021
Confluent	Confluent for Kubernetes	N/A	Not Affected		December 2021 Log4j Vulnerabilities Advisory			12/17/2021
Confluent	Confluent Kafka Connectors	N/A	Not Affected	N/A	December 2021 Log4j Vulnerabilities Advisory			12/17/2021
Confluent	Confluent ElasticSearch Sink Connector	<11.1.7	Affected	Yes	December 2021 Log4j Vulnerabilities Advisory			12/17/2021
Confluent	Confluent Google DataProc Sink	<1.1.5	Affected	Yes	December 2021 Log4j Vulnerabilities Advisory			12/17/2021
Confluent	Connector Confluent Splunk Sink Connector	< 2.05	Affected	Yes	December 2021 Log4j Vulnerabilities Advisory			12/17/2021
Confluent	Confluent HDFS 2 Sink Connector	<10.1.3	Affected	Yes	December 2021 Log4j Vulnerabilities Advisory			12/17/2021
Confluent	Confluent HDFS 3 Sink	<1.1.8	Affected		December 2021 Log4j Vulnerabilities Advisory			12/17/2021
Confluent	Connector Confluent VMWare Tanzu GemFire Sink Connector	<1.0.8	Affected	Yes	December 2021 Log4j Vulnerabilities Advisory			12/17/2021
Connect2id ConnectWise  ContrastSecuri ControlUp COPADATA  CouchBase CPanel Cradlepoint Crestron CrushFTP	ity		Not Affected		Connect2id Blog Post ConnectWise Advisory Link ContrastSecurity Article ControlUp Link COPADATA Support Services CouchBase Forums CPanel Forms Cradlepoint Crestron Advisory CrushFTP Link			12/20/2021
CryptShare					Cryptshare Support Link			
CyberArk	Privileged Threat Analytics (PTA)	N/A	Fixed	Yes	CyberArk Customer Force		This advisory is available to customers only and has not been reviewed by CISA.	12/14/2021
Cybereason CyberRes	, ,				Cybereason Blog Post CyberRes Community Link			
DarkTrace					DarkTrace Customer Portal			
Dassault Systèmes Databricks Datadog	Datadog Agent	>=6.17.0, <=6.32.2, >=7.17.0, <=7.32.2	Fixed	Yes	Databricks Google Doc Datadog Log4j Vulnerability Update			
Dataminer		×-1.11.0, ×-1.02.2			Dataminer Community Link			
Datev Datto dCache.org Debian Deepinstinct					Datev Community Link Datto Link dCache.org Link Debian Tracker Link Deepinstinct Link			

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

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

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

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated	
Dell	Dell Hybrid Client	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code		12/15/2021	
					Execution Vulnerability			
Dell	Dell	N/A	Not Affected	N/A	(CVE-2021-44228) Dell Response to Apache		12/15/2021	
2011	ImageAssist	1./11	1100 111100000	1./11	Log4j Remote Code		12/10/2021	
					Execution Vulnerability			
Dell	Dell Insights	N/A	Not Affected	N/A	(CVE-2021-44228) Dell Response to Apache		12/15/2021	
JCII	Client	11/11	1100 Tillected	11/11	Log4j Remote Code		12/10/2021	
					Execution Vulnerability			
Dell	Dell Linux	N/A	Not Affected	N/Δ	(CVE-2021-44228) Dell Response to Apache		12/15/2021	
Den	Assistant	11/11	1100 Milected	11/11	Log4j Remote Code		12/10/2021	
					Execution Vulnerability			
Dell	Dell Mobile	N/A	Not Affected	N / A	(CVE-2021-44228) Dell Response to Apache		12/15/2021	
Jen -	Connect	N/A	Not Affected	N/A	Log4j Remote Code		12/13/2021	
					Execution Vulnerability			
N 11	D II M '	DT / A	NI A CC 4 1	NT / A	(CVE-2021-44228)		19/17/2001	
Oell	Dell Monitor ISP	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code		12/15/2021	
	(Windows/Mac/L	inux)			Execution Vulnerability			
. 11	D. II.M.	27 / 4	N	27/4	(CVE-2021-44228)		10/17/0001	
Dell	Dell Monitor SDK	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code		12/15/2021	
	SDR				Execution Vulnerability			
					(CVE-2021-44228)			
ell	Dell Networking X-Series	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code		12/15/2021	
	A-Series				Execution Vulnerability			
					(CVE-2021-44228)			
Pell	Dell Open	N/A	Not Affected	N/A	Dell Response to Apache		12/15/2021	
	Manage Mobile				Log4j Remote Code Execution Vulnerability			
					(CVE-2021-44228)			
ell	Dell Open	N/A	Not Affected	N/A	Dell Response to Apache		12/15/2021	
	Manage Server Administrator				Log4j Remote Code Execution Vulnerability			
					(CVE-2021-44228)			
Dell	Dell	N/A	Not Affected	N/A	Dell Response to Apache		12/15/2021	
	OpenManage Change				Log4j Remote Code Execution Vulnerability			
	Management				(CVE-2021-44228)			
ell	Dell	N/A	Not Affected	N/A	Dell Response to Apache		12/15/2021	
	OpenManage Enterprise				Log4j Remote Code Execution Vulnerability			
	Power Manager				(CVE-2021-44228)			
.,	Plugin	37/4		27/4	,		and the land	
Dell	Dell Optimizer	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code		12/15/2021	
					Execution Vulnerability			
					(CVE-2021-44228)			
Dell	Dell OS	N/A	Not Affected	N/A	Dell Response to Apache		12/15/2021	
	Recovery Tool				Log4j Remote Code Execution Vulnerability			
					(CVE-2021-44228)			
Dell	Dell Peripheral	N/A	Not Affected	N/A	Dell Response to Apache		12/15/2021	
	Manager 1.4 / 1.5 for Windows				Log4j Remote Code Execution Vulnerability			
	1.0 201 11 maows				(CVE-2021-44228)			
Dell	Dell Platform	N/A	Not Affected	N/A	Dell Response to Apache		12/15/2021	
	Service				Log4j Remote Code Execution Vulnerability	,		
					(CVE-2021-44228)			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other	References	Last Updated
Dell	Dell Power	N/A	Not Affected	N/A	Dell Response to Apache			12/15/2021
	Manager				Log4j Remote Code			
					Execution Vulnerability			
D 11	D II D	NT / A	NI A C A 1	NI / A	(CVE-2021-44228)			10/15/0001
Dell	Dell Power	N/A	Not Affected	N/A	Dell Response to Apache			12/15/2021
	Manager Lite				Log4j Remote Code Execution Vulnerability			
					(CVE-2021-44228)			
Dell	Dell Precision	N/A	Not Affected	N/A	Dell Response to Apache			12/15/2021
Jon	Optimizer	11/11	1100 Tinecoca	11/11	Log4j Remote Code			12/10/2021
	Optimizer				Execution Vulnerability			
					(CVE-2021-44228)			
Dell	Dell Precision	N/A	Not Affected	N/A	Dell Response to Apache			12/15/2021
	Optimizer for	,		,	Log4j Remote Code			, ,
	Linux				Execution Vulnerability			
					(CVE-2021-44228)			
Dell	Dell Premier	N/A	Not Affected	N/A	Dell Response to Apache			12/15/2021
	Color				Log4j Remote Code			
					Execution Vulnerability			
					(CVE-2021-44228)			
Dell	Dell Recovery	N/A	Not Affected	N/A	Dell Response to Apache			12/15/2021
	(Linux)				Log4j Remote Code			
					Execution Vulnerability			
D 11	D 11	37/4	NT + 1 (C + 1	27/4	(CVE-2021-44228)			10/15/0001
Dell	Dell	N/A	Not Affected	N/A	Dell Response to Apache			12/15/2021
	Remediation				Log4j Remote Code			
	Platform				Execution Vulnerability			
Dell	Dell Remote	N/A	Not Affected	NI / A	(CVE-2021-44228)			19/15/2021
Jen	Execution Execution	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code			12/15/2021
	Engine				Execution Vulnerability			
	(DRONE)				(CVE-2021-44228)			
Dell	Dell Security	N/A	Not Affected	N/A	Dell Response to Apache			12/15/2021
Dell	Advisory	11/11	1100 IIIIccoca	11/11	Log4j Remote Code			12/10/2021
	Update -				Execution Vulnerability			
	DSA-2021-088				(CVE-2021-44228)			
Dell	Dell Security	N/A	Not Affected	N/A	Dell Response to Apache			12/15/2021
	Management	,		,	Log4j Remote Code			, ,
	Server & Dell				Execution Vulnerability			
	Security				(CVE-2021-44228)			
	Management				·			
	Server Virtual*							
Dell	Dell	N/A	Not Affected	N/A	Dell Response to Apache			12/15/2021
	SupportAssist				Log4j Remote Code			
	SOS				Execution Vulnerability			
	D. II	37/4		27/4	(CVE-2021-44228)			4.5 ( (
Dell	Dell Thin OS	N/A	Not Affected	N/A	Dell Response to Apache			12/15/2021
					Log4j Remote Code			
					Execution Vulnerability			
Dell	Dell Threat	N/A	Not A # 1	NI / A	(CVE-2021-44228)			19/15/2021
Den	Defi Threat Defense	N/A	Not Affected	IN/A	Dell Response to Apache Log4j Remote Code			12/15/2021
	Detense				Execution Vulnerability			
					(CVE-2021-44228)			
Dell	Dell True Color	N/A	Not Affected	N/A	Dell Response to Apache			12/15/2021
J011	Don True Color	11/11	1100 Illiected	11/11	Log4j Remote Code			12/10/2021
					Execution Vulnerability			
					(CVE-2021-44228)			
Dell	Dell Trusted	N/A	Not Affected	N/A	Dell Response to Apache			12/15/2021
- <del>-</del>	Device	, -		,	Log4j Remote Code			//
					Execution Vulnerability			
					(CVE-2021-44228)			
Dell	Dell Update	N/A	Not Affected	N/A	Dell Response to Apache			12/15/2021
	•	,		,	Log4j Remote Code			, ,
					Execution Vulnerability			

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

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	SmartByte	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code			12/15/2021
					Execution Vulnerability			
<b>.</b>	03 57 G	27/4		27/4	(CVE-2021-44228)			10/17/2001
Dell	SMI-S	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code			12/15/2021
					Execution Vulnerability			
					(CVE-2021-44228)			
Dell	Software RAID	N/A	Not Affected	N/A	Dell Response to Apache			12/15/2021
					Log4j Remote Code			
					Execution Vulnerability (CVE-2021-44228)			
Dell	Solutions	N/A	Not Affected	N/A	Dell Response to Apache			12/15/2021
	Enabler	,		,	Log4j Remote Code			, ,
					Execution Vulnerability			
Dell	Solutions	N/A	Not Affected	NI / A	(CVE-2021-44228) Dell Response to Apache			12/15/2021
Den	Enabler vApp	N/A	Not Affected	N/A	Log4j Remote Code			12/13/2021
	Enaster vripp				Execution Vulnerability			
					(CVE-2021-44228)			
Dell	Sonic	N/A	Not Affected	N/A	Dell Response to Apache			12/15/2021
					Log4j Remote Code			
					Execution Vulnerability (CVE-2021-44228)			
Dell	SRS VE	N/A	Not Affected	N/A	Dell Response to Apache			12/15/2021
		,		,	Log4j Remote Code			, ,
					Execution Vulnerability			
D-11	Ct Ct	NT / A	N-+ A (f+-1	NT / A	(CVE-2021-44228)			19/15/9091
Dell	Storage Center OS and	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code			12/15/2021
	additional SC				Execution Vulnerability			
	applications				(CVE-2021-44228)			
	unless otherwise							
D-11	noted	NT / A	N-+ A (f+-1	NT / A	D-11 D t- Al-			19/15/2021
Dell	$\begin{array}{c} { m SupportAssist} \\ { m Client} \end{array}$	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code			12/15/2021
	Commercial				Execution Vulnerability			
	0 01111101 0101				(CVE-2021-44228)			
Dell	SupportAssist	N/A	Not Affected	N/A	Dell Response to Apache			12/15/2021
	Client				Log4j Remote Code			
	Consumer				Execution Vulnerability (CVE-2021-44228)			
Dell	UCC Edge	N/A	Not Affected	N/A	Dell Response to Apache			12/15/2021
	000 2480	/	1.00 111100000	/	Log4j Remote Code			//
					Execution Vulnerability			
D 11	TT . 1 . C	DT / A	37 . A.C 1	37/4	(CVE-2021-44228)			10/17/0001
Dell	Unisphere for PowerMax	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code			12/15/2021
	FowerMax				Execution Vulnerability			
					(CVE-2021-44228)			
Dell	Unisphere for	N/A	Not Affected	N/A	Dell Response to Apache			12/15/2021
	PowerMax				Log4j Remote Code			
	vApp				Execution Vulnerability			
Dell	Unisphere for	N/A	Not Affected	N/A	(CVE-2021-44228) Dell Response to Apache			12/15/2021
Den	VMAX	11/11	Not Thected	11/11	Log4j Remote Code			12/10/2021
					Execution Vulnerability			
D 11	**	27/4		27/4	(CVE-2021-44228)			4-4
Dell	Unisphere for	N/A	Not Affected	N/A	Dell Response to Apache			12/15/2021
	VNX				Log4j Remote Code Execution Vulnerability			
					(CVE-2021-44228)			
Dell	Update	N/A	Not Affected	N/A	Dell Response to Apache			12/15/2021
	Manager Plugin	,		,	Log4j Remote Code			, ,
	-				Execution Vulnerability (CVE-2021-44228)			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	ViPR Controller	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability			12/15/2021
Dell	VNX1	N/A	Not Affected	N/A	(CVE-2021-44228) Dell Response to Apache			12/15/2021
					Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			
Dell	VNX2	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability			12/15/2021
		27/1		27/1	(CVE-2021-44228)			
Dell	VPLEX VS2/VS6 / VPLEX Witness	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability			12/15/2021
Dell	Vsan Ready Nodes	N/A	Not Affected	N/A	(CVE-2021-44228) Dell Response to Apache Log4j Remote Code			12/15/2021
					Execution Vulnerability (CVE-2021-44228)			
Dell	Warnado MLK (firmware)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability			12/15/2021
Dell	Wyse	N/A	Not Affected	N/A	(CVE-2021-44228) Dell Response to Apache			12/15/2021
	Proprietary OS (ThinOS)				Log4j Remote Code Execution Vulnerability (CVE-2021-44228)			
Dell	Wyse Windows Embedded Suite	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code			12/15/2021
D 11	ADEN G	27/4	Tr. 1	27/4	Execution Vulnerability (CVE-2021-44228)	CI. I		40/47/0004
Dell	APEX Console	N/A	Fixed	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability	Cloud environment patched		12/15/2021
Dell	APEX Data Storage Services		Affected	No	(CVE-2021-44228) Dell Response to Apache Log4j Remote Code	Cloud environment		12/15/2021
					Execution Vulnerability (CVE-2021-44228)	patch in progress		
Dell	Cloud IQ		Fixed	N/A	Dell Response to Apache Log4j Remote Code	Cloud environment		12/15/2021
					Execution Vulnerability (CVE-2021-44228)	patched		
Dell	Connectrix (Cisco MDS DCNM)		Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability	Patch expected by		12/15/2021
Dell	Connectrix	2.1.1	Affected	No	(CVE-2021-44228) Dell Response to Apache	12/23/21 Patch		12/15/2021
	B-Series SANnav				Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	expected by 3/31/2022		
Dell	Data Domain OS	Versions between 7.3.0.5 and 7.7.0.6; Versions	Affected	Yes	Dell Response to Apache Log4j Remote Code	See DSA- 2021-274		12/15/2021
		before 7.6.0.30			Execution Vulnerability (CVE-2021-44228)			
Dell	Dell EMC Avamar	"18.2 19.1 19.2 19.3 19.4"	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability	Patch expected by		12/15/2021
Dell	Dell EMC BSN		Affected	Yes	(CVE-2021-44228) Dell Response to Apache	12/20/21 See DSA-		12/15/2021
	Controller Node				Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	2021-305		
Dell	Dell EMC Cloud Disaster	N/A	Affected	No	Dell Response to Apache Log4j Remote Code	Patch pending		12/15/2021
	Recovery				Execution Vulnerability (CVE-2021-44228)			

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

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Dell	VxBlock		Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	"Patch pending See vce6771 (requires customer	12/15/2021
Dell	vRealize Orchestrator (vRO) Plug-ins for Dell EMC	Various	Affected		Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	login)" See DSA- 2021-300	12/15/2021
Dell	Storage vRO Plugin for Dell EMC PowerMax	Version 1.2.3 or earlier	Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability	See DSA- 2021-300	12/15/2021
Dell	vRO Plugin for Dell EMC PowerScale	Version 1.1.0 or earlier	Affected	Yes	(CVE-2021-44228) Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	See DSA- 2021-300	12/15/2021
Dell	vRO Plugin for Dell EMC PowerStore	Version 1.1.4 or earlier	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	See DSA- 2021-300	12/15/2021
Dell	vRO Plugin for Dell EMC Unity	Version 1.0.6 or earlier	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	See DSA- 2021-300	12/15/2021
Dell	vRO Plugin for Dell EMC XtremIO	Version 4.1.2 or earlier	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	See DSA- 2021-300	12/15/2021
Dell	vRealize Data Protection Extension Data Management		Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch expected by 12/19/21	12/15/2021
Dell	vRealize Data Protection Extension for vRealize Automation (vRA) 8.x	"version 19.6 version 19.7 version 19.8 and version 19.9"	Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch expected by 12/19/21	12/15/2021
Dell	VMware vRealize Automation 8.x	" $8.2\ 8.3\ 8.4\ 8.5\ \mathrm{and}\ 8.6$ "	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)	Patch expected by 12/19/21	12/15/2021
Dell	VMware vRealize Orchestrator 8.x	" $8.2\ 8.3\ 8.4\ 8.5\ \mathrm{and}\ 8.6$ "	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)		12/15/2021
Dell	Wyse Management Suite	<3.5	Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)		12/15/2021
Deltares	Delft-FEWS	>2018.02	Fixed	No	Deltares Advisory	Mitigations Only	12/22/2021
Denequa Device42 Devolutions	All products		Not Affected		Denequa Link Device42 Link https: //blog.devolutions.net/ 2021/12/critical- vulnerability-in-log4j/	Ошу	
Diebold Nixdorf	OTDIZ Gasas		N / AC · ·		Diebold Nixdorf Link		10/01/0007
Digi International	CTEK G6200 family CTEK		Not Affected Not Affected		Digi International Advisory Link Digi International		12/21/2021 $12/21/2021$

Vendor	Product	Version(s) Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Digi International	CTEK Z45 family	Not Affected		Digi International Advisory Link			12/21/2021
Digi	Digi 54xx family	Not Affected		Digi International			12/21/2021
International Digi	Digi 63xx family	Not Affected		Advisory Link Digi International			12/21/2021
International Digi	Digi	Not Affected		Advisory Link Digi International			12/21/2021
International	AnywhereUSB (G2) family			Advisory Link			, ,
Digi	Digi	Not Affected		Digi International			12/21/2021
International	AnywhereUSB Plus family			Advisory Link			
Digi International	Digi Connect family	Not Affected		Digi International Advisory Link			12/21/2021
Digi	Digi Connect	Not Affected		Digi International			12/21/2021
International Digi	EZ family Digi Connect IT	Not Affected		Advisory Link Digi International			12/21/2021
International Digi	family Digi	Not Affected		Advisory Link Digi International			12/21/2021
International	ConnectPort	Not Affected		Advisory Link			12/21/2021
Digi	family Digi	Not Affected		Digi International			12/21/2021
International	ConnectPort LTS family	1100 111100000		Advisory Link			,,
Digi	Digi Connect	Not Affected		Digi International			12/21/2021
International Digi	Sensor family Digi Connect	Not Affected		Advisory Link Digi International			12/21/2021
International	WS family			Advisory Link			
Digi International	Digi Embedded Android	Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi Embedded Yocto	Not Affected		Digi International Advisory Link			12/21/2021
Digi	Digi EX routers	Not Affected		Digi International			12/21/2021
International Digi	Digi IX routers	Not Affected		Advisory Link Digi International			12/21/2021
International Digi	Digi LR54	Not Affected		Advisory Link Digi International			12/21/2021
International				Advisory Link			, ,
Digi International	Digi One family	Not Affected		Digi International Advisory Link			12/21/2021
Digi International	Digi Passport family	Not Affected		Digi International Advisory Link			12/21/2021
Digi	Digi PortServer	Not Affected		Digi International			12/21/2021
International Digi	TS family Digi TX routers	Not Affected		Advisory Link Digi International			12/21/2021
International		Not Affected		Advisory Link			, ,
Digi International	Digi WR11			Digi International Advisory Link			12/21/2021
Digi International	Digi WR21	Not Affected		Digi International Advisory Link			12/21/2021
Digi	Digi WR31	Not Affected		Digi International			12/21/2021
International Digi	Digi	Not Affected		Advisory Link Digi International			12/21/2021
International Digi	WR44R/RR Digi WR54	Not Affected		Advisory Link Digi International			12/21/2021
International				Advisory Link			
Digi International	Digi WR64	Not Affected		Digi International Advisory Link			12/21/2021
Digi International	AnywhereUSB Manager	Not Affected		Digi International Advisory Link			12/21/2021
Digi	Aview	Not Affected		Digi International			12/21/2021
International Digi	ARMT	Not Affected		Advisory Link Digi International			12/21/2021
International Digi	AVWOB	Not Affected		Advisory Link Digi International			12/21/2021
International				Advisory Link			
Digi International	Digi Navigator	Not Affected		Digi International Advisory Link			12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
igi	Digi Remote		Not Affected		Digi International			12/21/2021
iternational	Manager				Advisory Link			
Digi	Digi Xbee		Not Affected		Digi International			12/21/2021
nternational	mobile app				Advisory Link			
igi	Lighthouse		Not Affected		Digi International			12/21/2021
nternational					Advisory Link			
igi	Realport		Not Affected		Digi International			12/21/2021
nternational					Advisory Link			
igi	Remote Hub		Not Affected		Digi International			12/21/2021
nternational	Config Utility				Advisory Link			
igicert					Digicert Link			
igital AI					Digital AI Article			
NSFilter					DNSFilter Blog Post			
ocker					Docker Blog Post			
ocusign					Docusign Alert			
)rayTek	Vigor Routers,		Not Affected		DrayTek Statement			12/15/2021
	Access Points,							
	Switches,							
	VigorACS							
	Central							
	Management							
	Software,							
	MyVigor							
	Platform							
Space					DSpace Google Group			
ynatrace	Managed cluster		Not Affected	No	Official Dynatrace	Please see		12/21/2021
	nodes				Communication	Dynatrace		
						Communi-		
						cation for		
						details		
ynatrace	SAAS		Fixed	No	Official Dynatrace			12/21/2021
					Communication			
ynatrace	FedRamp SAAS		Fixed	No	Official Dynatrace			12/21/2021
					Communication			
ynatrace	Synthetic public		Fixed	No	Official Dynatrace			12/21/2021
	locations				Communication			
ynatrace	Synthetic		Fixed	Yes	Official Dynatrace	Please see		12/21/2021
	Private				Communication	Dynatrace		
	ActiveGate					Communi-		
						cation for		
			37 . 100	37	0.00	details		40/01/0001
)ynatrace	ActiveGate		Not Affected	No	Official Dynatrace			12/21/2021
			**	37	Communication			12 /24 /255
ynatrace	OneAgent		Not Affected	No	Official Dynatrace			12/21/2021
	_			(0 )	Communication			
ynatrace	Dynatrace		Fixed	Yes (See Notes)	Official Dynatrace	Please see		12/21/2021
	Extensions				Communication	Dynatrace		
						Communi-		
						cation for		
ъ					D D :	details		
asyRedmine					EasyRedmine News			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Eaton	Undisclosed	Undisclosed	Affected		Security Bulletin	Doesn't openly		
						disclose		
						what		
						products		
						are		
						affected or		
						not for		
						quote 'security		
						purposes'.		
						Needs		
						email regis-		
						tration.		
						No workaround		
						provided		
						due to reg-		
						istration		
						wall.		
EclecticIQ					EclecticIQ Advisory			
Eclipse Foundation					Eclipse Foundation Wiki			
EFI					EFI Link			
EGroupware					EGroupware Link			
Elastic	APM Java		$\operatorname{Under}$		Apache Log4j2 Remote			12/15/2021
	Agent		Investigation		Code Execution (RCE)			
					Vulnerability - CVE-2021-44228 -			
					ESA-2021-44228 - ESA-2021-31			
Elastic	APM Server		Not Affected		Apache Log4j2 Remote			12/15/2021
					Code Execution (RCE)			,,
					Vulnerability -			
					CVE-2021-44228 -			
T21	D. A		NI ACC		ESA-2021-31			10/17/2021
Elastic	Beats		Not Affected		Apache Log4j2 Remote Code Execution (RCE)			12/15/2021
					Vulnerability -			
					CVE-2021-44228 -			
					ESA-2021-31			
Elastic	$\operatorname{Cmd}$		Not Affected		Apache Log4j2 Remote			12/15/2021
					Code Execution (RCE)			
					Vulnerability - CVE-2021-44228 -			
					ESA-2021-31			
Elastic	Elastic Agent		Not Affected		Apache Log4j2 Remote			12/15/2021
					Code Execution (RCE)			, ,
					Vulnerability -			
					CVE-2021-44228 -			
Elastic	Elastic Cloud		Under		ESA-2021-31 Apache Log4j2 Remote			12/15/2021
Liasuc	Enterprise		Investigation		Code Execution (RCE)			12/10/2021
	<u> </u>		in ostigation		Vulnerability -			
					CVE-2021-44228 -			
					ESA-2021-31			
Elastic	Elastic Cloud		Under		Apache Log4j2 Remote			12/15/2021
	Enterprise		Investigation		Code Execution (RCE) Vulnerability -			
					Vumerability - CVE-2021-44228 -			
					ESA-2021-31			
Elastic	Elastic Cloud		Not Affected		Apache Log4j2 Remote			12/15/2021
	on Kubernetes				Code Execution (RCE)			
					Vulnerability -			
					CVE-2021-44228 -			
					ESA-2021-31			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Elastic	Elastic Cloud		Under Investigation		Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 -		12/15/2021
Elastic	Elastic Endgame		Not Affected		ESA-2021-31 Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 -		12/15/2021
Elastic	Elastic Maps Service		Not Affected		ESA-2021-31 Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 -		12/15/2021
Elastic	Elasticsearch	5,6,8	Affected	Yes	ESA-2021-31 Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 -		12/15/2021
Elastic	Endpoint Security		Not Affected		ESA-2021-31 Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 -		12/15/2021
Elastic	Enterprise Search		Not Affected		ESA-2021-31 Apache Log4j2 Remote Code Execution (RCE) Vulnerability -		12/15/2021
Elastic	Fleet Server		Not Affected		CVE-2021-44228 - ESA-2021-31 Apache Log4j2 Remote Code Execution (RCE) Vulnerability -		12/15/2021
Elastic	Kibana		Not Affected		CVE-2021-44228 - ESA-2021-31 Apache Log4j2 Remote Code Execution (RCE) Vulnerability -		12/15/2021
Elastic	Logstash	<6.8.21,<7.16.1	Affected	Yes	CVE-2021-44228 - ESA-2021-31 Apache Log4j2 Remote Code Execution (RCE) Vulnerability -		12/15/2021
Elastic	Machine Learning		Not Affected		CVE-2021-44228 - ESA-2021-31 Apache Log4j2 Remote Code Execution (RCE) Vulnerability -		12/15/2021
Elastic	Swiftype		Not Affected		CVE-2021-44228 - ESA-2021-31 Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 -		12/15/2021
ElasticSearch	all products		Not Affected		ESA-2021-31		
Ellucian	Banner Analytics		Affected	No	Ellucian Response on Apache Log4j Issue		12/17/2021
Ellucian	Colleague		Affected	No	Ellucian Response on Apache Log4j Issue	On-prem and cloud deploye- ments expect fixed 12/18/2021	12/17/2021
Ellucian	Admin		Not Affected		Ellucian Response on Apache Log4j Issue	12/10/2021	12/17/2021

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

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Emerson	Gas Chro-		Not Affected		Emerson Security			12/17/2021
	matographs:				Notification			
	M500/2350A				EMR.RMT21003-2			
	MON2000 700XA/1500XA							
	370XA							
	MON2020							
Emerson	Gas Analysis:		Not Affected		Emerson Security			12/17/2021
	X-STREAM				Notification			
	Enhanced (VECD VECK				EMR.RMT21003-2			
	(XEGP XEGK XEGC XEGF							
	XEGC XEGF XEFD XECLD)							
Emerson	Gas Detection:		Not Affected		Emerson Security			12/17/2021
	Millennium II				Notification			, ,
	Basic Single &				EMR.RMT21003-2			
	Dual Channel 928 Wireless							
	Gas Wireless							
	Monitor/628							
	Gas Sensor 935							
	&936 Open							
	Path Gas							
	Detector Millennium Air							
	Particle Monitor							
Emerson	Incus Ultrasonic		Not Affected		Emerson Security			12/17/2021
	gas leak				Notification			, ,
	detector				EMR.RMT21003-2			
Emerson	Flame		Not Affected		Emerson Security			12/17/2021
	Detection: 975UF &				Notification EMR.RMT21003-2			
	975UR Infrared				EMIR.RMI 1 21003-2			
	Flame Detectors							
	975HR Infrared							
	Hydrogen Flame							
	Detector 975MR							
	Multi-Spectrum Infrared Flame							
	Detector							
Emerson	Liquid		Not Affected		Emerson Security			12/17/2021
	Transmitters:				Notification			
	5081 1066 1056				EMR.RMT21003-2			
Emerson	1057 56 Combustion:		Not Affected		Emerson Security			12/17/2021
Emerson	OCX OXT 6888		Not Affected		Notification			12/11/2021
	CX1100 6888Xi				EMR.RMT21003-2			
Emerson	Spectrex family		Not Affected		Emerson Security			12/17/2021
	Flame Detectors				Notification			
	and Rosemount 975 flame				EMR.RMT21003-2			
	detector							
Emerson	CT4400 QCL		Not Affected		Emerson Security			12/17/2021
	General				Notification			, ,
	Purpose				EMR.RMT21003-2			
	Continuous Gas							
Emerson	Analyzer CT5400 QCL		Not Affected		Emerson Security			12/17/2021
Emerson	General		Not Affected		Notification			12/11/2021
	Purpose				EMR.RMT21003-2			
	Continuous Gas							
	Analyzer							
Emerson	CT5100 QCL		Not Affected		Emerson Security			12/17/2021
	Field Housing Continuous Gas				Notification EMR.RMT21003-2			
	Analyzer				121V11V-1V1V1 1 2 1 UU 0-2			

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Emerson	326T		Not Affected		Emerson Security			12/17/2021
	Temperature				Notification			
	Transmitter				EMR.RMT21003-2			
Emerson	327T		Not Affected		Emerson Security			12/17/2021
	Temperature				Notification			
T.	Transmitter		27 . 1		EMR.RMT21003-2			40/47/0004
Emerson	648		Not Affected		Emerson Security			12/17/2021
	Temperature				Notification			
_	Transmitter		37 . 100 . 1		EMR.RMT21003-2			10 117 10001
Emerson	4088 Upgrade		Not Affected		Emerson Security			12/17/2021
	Utility				Notification			
			27 . 1		EMR.RMT21003-2			40/47/0004
Emerson	Engineering		Not Affected		Emerson Security			12/17/2021
	Assistant 5.x &				Notification			
	6.x		27 . 1		EMR.RMT21003-2			40/47/0004
Emerson	248		Not Affected		Emerson Security			12/17/2021
	Configuration				Notification			
_	Application				EMR.RMT21003-2			
Emerson	Rosemount		Not Affected		Emerson Security			12/17/2021
	IO-Link				Notification			
	Assistant				EMR.RMT21003-2			
Emerson	Rosemount		Not Affected		Emerson Security			12/17/2021
	TankMaster and				Notification			
	TankMaster				EMR.RMT21003-2			
	Mobile							
Emerson	Rosemount		Not Affected		Emerson Security			12/17/2021
	RadarMaster				Notification			
	and				EMR.RMT21003-2			
	RadarMaster							
	Plus							
Emerson	Rosemount		Not Affected		Emerson Security			12/17/2021
	Radar				Notification			
	Configuration				EMR.RMT21003-2			
	Tool							
Emerson	Rosemount 2460		Not Affected		Emerson Security			12/17/2021
	System Hub				Notification			
					EMR.RMT21003-2			
Emerson	Rosemount 2410		Not Affected		Emerson Security			12/17/2021
	Tank Hub				Notification			
					EMR.RMT21003-2			
Emerson	Rosemount 3490		Not Affected		Emerson Security			12/17/2021
	Controller				Notification			
					EMR.RMT21003-2			
Emerson	Rosemount 2230		Not Affected		Emerson Security			12/17/2021
	Graphical Field				Notification			
	Display				EMR.RMT21003-2			
Emerson	Rosemount		Not Affected		Emerson Security			12/17/2021
	2240S				Notification			
	Multi-input				EMR.RMT21003-2			
	Temperature							
	Transmitter							
Emerson	Rosemount		Not Affected		Emerson Security			12/17/2021
	CMS/SCU				Notification			
	51/SCC				EMR.RMT21003-2			
Emerson	Rosemount		Not Affected		Emerson Security			12/17/2021
	CMS/WSU				Notification			
	51/SWF 51				EMR.RMT21003-2			
Emerson	Rosemount		Not Affected		Emerson Security			12/17/2021
	CMS/IOU 61				Notification			• •
	,				EMR.RMT21003-2			
Emerson	Rosemount		Not Affected		Emerson Security			12/17/2021
	Level				Notification			, ,
					EMR.RMT21003-2			
	Transmitters							
	Transmitters (14xx 33xx 53xx				EMIC.ICM121000 2			

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
ESRI	ArcGIS Server	All	Fixed	Yes	https:	Requires		12/17/2021
					//www.esri.com/arcgis-	script re-		
					blog/products/arcgis-	mediation.		
					enterprise/	ESRI has		
					administration/arcgis-	created		
					software-and-cve-2021-	scripts to		
					44228-aka-log4shell-aka-	remove the		
					$\log$ jam/	JndiLookup		
						class, but		
						has not		
						issued		
						patches to		
						upgrade		
						the Log4j versions		
ESRI	$\operatorname{ArcGIS}$	All	Fixed	Yes	https:	Requires		12/17/2021
ESIT	Workflow	All	Fixed	165	//www.esri.com/arcgis-	script re-		12/11/2021
	Manager Server				blog/products/arcgis-	mediation.		
	Manager Server				enterprise/	ESRI has		
					administration/arcgis-	created		
					software-and-cve-2021-	scripts to		
					44228-aka-log4shell-aka-	remove the		
					logjam/	JndiLookup		
					logJulii/	class, but		
						has not		
						issued		
						patches to		
						upgrade		
						the Log4j		
						versions		
ESRI	Portal for	All	Fixed	Yes	https:	Requires		12/17/2021
	$\operatorname{ArcGIS}$				//www.esri.com/arcgis-	script re-		
					blog/products/arcgis-	mediation.		
					enterprise/	ESRI has		
					administration/arcgis-	created		
					software-and-cve-2021-	scripts to		
					44228-aka-log4shell-aka-			
					$\log$ jam/	JndiLookup	1	
						class, but		
						has not		
						issued		
						patches to		
						upgrade the Log4j		
						versions		
Estos					Estos Support	VELSIOHS		
10000					Statement			
Evolveum					Evolveum Midpoint			
Midpoint					Statement			
Ewon					Ewon Statement			
Exabeam					Exabeam Statement	This		
						advisory is		
						available		
						to		
						customers		
						only and		
						has not		
						been		
						reviewed		
						by CISA		
Exact					Exact Statement			
Exivity					Exivity Statement			
ExtraHop	Reveal(x)	<=8.4.6, <=8.5.3,	Affected	Yes	ExtraHop Statement	Versions		12/21/2021
		<=8.6.4				>8.4.7,		
						>8.5.4,		
						> 8.6.5 and		
						>=8.7  are		
						fixed.		
						nacu.		

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

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

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
lEx	Ship Manager	Unknown	Affected/Under		FedEx Statement	Note:		12/15/2021
	Software		Investigation			FedEx is		
						aware of		
						the issue		
						related to		
						the Log4j		
						Remote		
						Code		
						Execution		
						vulnerabil-		
						ity		
						affecting		
						various		
						Apache		
						products.		
						We are		
						actively		
						assessing		
						the		
						situation		
						and taking		
						necessary		
						action as		
						appropri-		
						ate. As a		
						result, we		
						are tem-		
						porarily		
					unable to			
						provide a		
						link to		
						download		
						the FedEx		
						Ship		
						Manager		
						software or		
						generate		
						product		
						keys needed for		
						registra-		
						tion of		
						FedEx		
						Ship		
						Manager		
						software.		
						We are		
						working to		
						have this		
						resolved as		
						quickly as		
						possible		
						and		
						apologize		
						for the		
						inconve-		
						nience.		
						For related		
						questions		
						or the		
						most		
						updated		
						informa-		
						tion,		
						customers		
						should		
						check		
						FedEx		
						Updates		
						for Apache		
					84	Log4;		
					<del>-</del>	Log4j Issue or		
						contact		
						their		
						their Customer		
						Technol-		
						ogy representati		

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Fortinet	${\bf FortiDeceptor}$		Not Affected		PSIRT Advisories			
Fortinet	FortiEDR Agent		Not Affected		FortiGuard PSIRT Advisories			
	101012210118011	•	1100 111100000		FortiGuard			
Fortinet	FortiEDR Cloud	l	Affected		PSIRT Advisories			
Fortinet	FortiGate Cloud	I	Not Affected		FortiGuard PSIRT Advisories			
OI tillet	TortiGate Cloud	L	Not Affected		FortiGuard			
ortinet	FortiGSLB		Not Affected		PSIRT Advisories			
lantin at	Cloud FortiMail		Not Affected		FortiGuard PSIRT Advisories			
ortinet	roruman		Not Affected		FortiGuard			
Fortinet	${\bf FortiManager}$		Not Affected		PSIRT Advisories			
74:4	E4:M		N-+ A.C+-1		FortiGuard PSIRT Advisories			
Fortinet	FortiManager Cloud		Not Affected		FortiGuard			
ortinet	FortiNAC		Affected		PSIRT Advisories			
					FortiGuard			
ortinet	FortiNAC		Affected		PSIRT Advisories FortiGuard			
ortinet	FortiOS		Not Affected		PSIRT Advisories			
	(includes				FortiGuard			
	FortiGate &							
Fortinet	FortiWiFi) FortiPhish		Not Affected		PSIRT Advisories			
	Cloud		1100 111100000		FortiGuard			
ortinet	FortiPolicy		Affected		PSIRT Advisories			
Fortinet	FortiPortal		Affected		FortiGuard PSIRT Advisories			
OI tillet	Forth Ortal		Allected		FortiGuard			
ortinet	${\bf FortiRecorder}$		Not Affected		PSIRT Advisories			
ortinet	FortiSIEM		Affected		FortiGuard PSIRT Advisories			
or timet	FOLUSTEM		Affected		FortiGuard			
ortinet	${\bf FortiSOAR}$		Affected		PSIRT Advisories			
	D 4:0 : 41		N A C 1		FortiGuard			
ortinet	FortiSwicth Cloud in		Not Affected		PSIRT Advisories FortiGuard			
	FortiLANCloud				1 of violating			
ortinet	FortiSwitch &		Not Affected		PSIRT Advisories			
ortinet	FortiSwitchMan FortiToken	ager	Not Affected		FortiGuard PSIRT Advisories			
or office	Cloud		Not Thected		FortiGuard			
ortinet	FortiVoice		Not Affected		PSIRT Advisories			
ortinet	FortiWeb Cloud		Not Affected		FortiGuard PSIRT Advisories			
orumer	Fortiweb Cloud	l	Not Affected		FortiGuard			
ortinet	ShieldX		Affected		PSIRT Advisories			
TA DI					FortiGuard			
TAPI Jujitsu					FTAPI Statement Fujitsu Statement			
usionAuth	FusionAuth	1.32	Not Affected		log4j CVE: How it			
					affects FusionAuth			
					(TLDR: It doesn't) - FusionAuth			
E Digital			Unknown		GE Digital Advisory	This		12/22/2021
G					Link(login required)	advisory is		, , , , , , , ,
						available		
						to customers		
						only and		
						has not		
						been		
						reviewed		

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

	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
GE Healthcare			Unknown		GE Healthcare Advisory Link	This advisory is		12/22/2021
						not		
						available		
						at the time of this		
						review,		
						due to		
						maintence		
						on the GE		
						Healthcare		
Gearset					Gearset Statement	website.		
Genesys					Genesys Statement			
GeoServer					GeoServer			
					Announcement			
Gerrit code review					Gerrit Statement			
GFI					GFI Statement			
Ghidra					Ghidra Statement			
Gigamon	Fabric Manager	< 5.13.01.02	Affected	Yes	Gigamon Customer	Updates		12/21/2021
					Support Portal	available via the		
						Gigamon		
						Support		
						Portal.		
						This		
						advisory		
						available		
						to customers		
						only and		
						has not		
						been		
						reviewed		
C:4IIb	$\operatorname{GitHub}$	CitII-la ann and	Fixed		GitHub Statement	by CISA.		19 /17 /9091
GitHub	Github	GitHub.com and GitHub Enterprise Cloud	Fixed		Github Statement			12/17/2021
GitLab					GitLab Statement			
Globus					Globus Statement			
GoAnywhere		< 6.8.6	Affected	Yes	GoAnywhere Statement			12/18/2021
		< 2.8.4	Affected	Yes	GoAnywhere Statement			12/18/2021
GoAnywhere	MH"I' Agents	< 1.6.5	Affected	Yes	GoAnywhere Statement			12/18/2021
GoAnywhere GoAnywhere	MI I Agentos				GoCD Statement			12/21/2021
GoAnywhere GoAnywhere GoCD			Not Affected		https://cloud.google	Product		
GoAnywhere GoAnywhere GoCD	AI Platform		Not Affected		https://cloud.google.	Product does not		12/21/2021
GoAnywhere GoAnywhere GoCD			Not Affected		com/log4j2-security-	does not		12/21/2021
GoAnywhere GoAnywhere GoCD	AI Platform		Not Affected		https://cloud.google. com/log4j2-security- advisory			12/21/2021
GoAnywhere GoAnywhere GoCD	AI Platform		Not Affected		com/log4j2-security-	does not use Log4j 2 and is not		12/21/2021
GoAnywhere GoAnywhere GoCD	AI Platform		Not Affected		com/log4j2-security-	does not use Log4j 2 and is not impacted		12/21/2021
GoAnywhere GoAnywhere GoCD	AI Platform		Not Affected		com/log4j2-security-	does not use Log4j 2 and is not impacted by the		12/21/2021
GoAnywhere GoAnywhere GoCD	AI Platform		Not Affected		com/log4j2-security-	does not use Log4j 2 and is not impacted by the issues		12/21/2021
GoAnywhere GoAnywhere GoCD	AI Platform		Not Affected		com/log4j2-security-	does not use Log4j 2 and is not impacted by the issues identified		12/21/2021
GoAnywhere GoAnywhere GoCD	AI Platform		Not Affected		com/log4j2-security-	does not use Log4j 2 and is not impacted by the issues identified in		12/21/2021
GoAnywhere GoAnywhere GoCD	AI Platform		Not Affected		com/log4j2-security-	does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-		12/21/2021
GoAnywhere GoAnywhere GoCD	AI Platform		Not Affected		com/log4j2-security-	does not use Log4j 2 and is not impacted by the issues identified in		12/21/2021

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

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

Vendor	Product V	Version(s) Status	Update Available	Vendor Link	Notes	Other References	Last Updated		
Google Cloud	Anthos Connect	Not Affected		https://cloud.google.	Product		12/21/2021		
				com/log4j2-security-	does not				
				advisory	use Log4j				
				v	2 and is				
					not				
					impacted				
					by the				
					issues				
					identified				
					$_{ m in}$				
					CVE-2021-				
					44228 and				
					CVE-2021-				
					45046.				
Google Cloud	Anthos Hub	Not Affected		https://cloud.google.	Product		12/21/2021		
Google Cloud	Alithos Hub	Not Affected		11. tps.//cioud.google.			12/21/2021		
				com/log4j2-security-	does not				
				advisory	use $Log4j$				
					2 and is				
					$\operatorname{not}$				
					impacted				
					by the				
					issues				
					identified				
					in				
				CVE-2021-					
				44228 and					
					CVE-2021-				
					45046.				
Google Cloud	Anthos Identity	Not Affected	Not Affected	https://cloud.google.	Product		12/21/2021		
O			Service			com/log4j2-security-	does not		, ,
	2011100			advisory	use Log4j				
				advisory	2 and is				
					not				
					impacted				
					by the				
					issues				
					identified				
					in				
					CVE-2021-				
					44228  and				
					CVE-2021-				
a . a	4				45046.		40/0-/000		
Google Cloud		Not Affected		https://cloud.google.	Product		12/21/2021		
	Premium			com/log4j2-security-	does not				
	Software			advisory	use $Log4j$				
				•	2 and is				
					not				
					impacted				
					hy the				
					by the				
					issues				
					identified				
					$_{ m in}$				
						CITIE 0001			
					CVE-2021-				
					CVE-2021- 44228 and CVE-2021-				

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Anthos Service Mesh		Not Affected		https://cloud.google. com/log4j2-security- advisory	Product does not use Log4j 2 and is		12/21/2021
						not impacted		
						by the issues		
						identified in		
						CVE-2021-		
						44228 and CVE-2021-		
Google Cloud	Anthos on		Not Affected		https://cloud.google.	45046. Product		12/21/2021
	VMWare				com/log4j2-security- advisory	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 recommen-		
						dations docu-		
						$\begin{array}{c} \mathrm{mented~in} \\ \mathrm{VMSA-} \end{array}$		
						2021-0028 and deploy		
						fixes or workaround	s	
						to their VMware		
						products as they		
						become available.		
						We also		
						recom- mend		
						customers review		
						their respective		
						applica- tions and		
						workloads affected by		
						the same vulnerabil-		
						ities and		
						apply appropriate		
						patches.		

	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
oogle Cloud	Apigee		Not Affected		https://cloud.google.	Apigee		12/17/2021
					com/log4j2-security-	installed		
					advisory	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		
						environ- ments to		
						identify		
						compo-		
						nents		
						dependent		
						on Log4j		
						and		
						update		
						them to		
						the latest		
						version.		
						Visit the		
						$egin{array}{c} { m Apigee} \\ { m Incident} \end{array}$		
						Incident		
						Report for more		

ndor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
ogle Cloud	App Engine		Not Affected		https://cloud.google.	Product		12/21/2021
					com/log4j2-security-	does not		
					advisory	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		
						environ-		
						ments to		
						identify		
						compo-		
						nents		
						dependent		
						on Log4j 2		
						and		
						update		
						them to		
						the latest		
						version.		

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

Vendor	Product Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Assured	Not Affected		https://cloud.google.	Product		12/21/2021
	Workloads			com/log4j2-security-	does not		
				advisory	use Log4j		
				·	2 and is		
					not		
					impacted		
					by the		
					issues		
					identified		
					in		
					CVE-2021-		
					44228 and		
					CVE-2021-		
G 1 G1 1	A N.	N		1 // 1 1 1	45046.		10/01/0001
Google Cloud	AutoML	Not Affected		https://cloud.google.	Product		12/21/2021
				com/log4j2-security-	does not		
				advisory	use $Log4j$		
					2 and is		
					not		
					impacted		
					by the		
					issues		
					identified		
					$_{ m in}$		
					CVE-2021-		
					44228 and		
					CVE-2021-		
					45046.		
Google Cloud	AutoMI.	Not Affected		https://cloud.google.	Product		12/21/2021
Google Cloud	Natural	Not Affected		com/log4j2-security-	does not		12/21/2021
				advisory	use Log4j		
	Language			advisory	2 and is		
					not		
					impacted		
					by the		
					issues		
					identified		
					$_{ m in}$		
					CVE-2021-		
					44228 and		
					CVE-2021-		
					45046.		
Google Cloud	AutoML Tables	Not Affected		https://cloud.google.	Product		12/21/2021
Ü				com/log4j2-security-	does not		, ,
				advisory	use Log4j		
				<i>yy</i>	2 and is		
					not		
					impacted		
					by the		
					issues		
					identified		
					in		
					CVE-2021-		
					44228 and		
					CIT ITT 0001		
					CVE-2021- 45046.		

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

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

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
oogle Cloud			Not Affected		https://cloud.google.	Product		12/15/2021
	Composer				com/log4j2-security-	does not		
					advisory	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 de-		
						pendencies		
						via DAGs,		
						installed		
						PyPI		
						modules,		
						plugins, or		
						other		
						services		
						that are		
						using		
						vulnerable		
						versions of		
						Log4j 2.		
						We		
						strongly		
						encourage		
						customers,		
						who		
						manage		
						Composer		
						environ-		
						ments to		
						identify		
						compo-		
						nents		
						dependent		
						on Log4j 2		
						and		
						update		
						them to		
						them to the latest version.		

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

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

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Cloud Logging		Not Affected		https://cloud.google.	Product		12/21/2021
					com/log4j2-security-	does not		
					advisory	use Log4j		
					J. L. C.	2 and is		
						not		
						impacted		
						by the		
						issues		
						identified		
						$_{ m in}$		
						CVE-2021-		
						44228  and		
						CVE-2021-		
						45046.		
Google Cloud	Cloud Network		Not Affected		https://cloud.google.	Product		12/20/2021
Google Cloud	Address		1100 Illicolou		com/log4j2-security-	does not		12/20/2021
					com/log4j2-security-			
	Translation				advisory	use Log4j		
	(NAT)					2 and is		
						not		
						impacted		
						by the		
						issues		
						identified		
						$_{ m in}$		
						CVE-2021-		
						44228 and		
						CVE-2021-		
						45046.		
C1 - C11	C11 N-41		N - + A C + - 1		1. + + / / - 1 1 1 -			19 /91 /9091
Google Cloud	Cloud Natural		Not Affected		https://cloud.google.	Product		12/21/2021
	Language API				com/log4j2-security-	does not		
					advisory	use $Log4j$		
						2 and is		
						$\operatorname{not}$		
						impacted		
						by the		
						issues		
						identified		
						in		
						CVE-2021-		
						44228 and		
						CVE-2021-		
						45046.		
Google Cloud	Cloud Profiler		Not Affected		https://cloud.google.	Product		12/21/2021
					com/log4j2-security-	does not		
					advisory	use Log4j		
						2 and is		
						$\operatorname{not}$		
						impacted		
						by the		
						issues		
						$_{\cdot}^{\mathrm{identified}}$		
						in		
						CVE-2021-		
						44228  and		
						CVE-2021-		

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Update
Google Cloud	Cloud Shell		Not Affected		https://cloud.google.	Product		12/21/2021
					com/log4j2-security-	does not		
					advisory	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 envi-		
						ronments		
						to identify		
						compo-		
						nents		
						dependent		
						on Log4j 2		
						and		
						update		
						them to		
						the latest		
						version.		
Google Cloud	Cloud Source		Not Affected		https://cloud.google.	Product		12/21/2021
	Repositories				com/log4j2-security-	does not		
					advisory	use Log4j		
						2 and is		
						$\operatorname{not}$		
						impacted		
						by the		
						issues		
						identified		
						racminied		
						in		
						in CVE-2021-		
						in		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Cloud Spanner		Not Affected		https://cloud.google.	Product		12/19/2021
					com/log4j2-security-	does not		
					advisory	use $Log4j$		
					v	2 and is		
						not		
						impacted		
						by the		
						issues		
						identified		
						in		
						CVE-2021-		
						44228 and		
						CVE-2021-		
						45046.		
Google Cloud	Cloud Storage		Not Affected		https://cloud.google.	Product		12/20/2021
					com/log4j2-security-	does not		
					advisory	use Log4j		
						2 and is		
						not		
						impacted		
						by the		
						issues		
						identified		
						in		
						CVE-2021-		
						44228 and		
						CVE-2021-		
	C1 1.T2 1		27 . 100 . 1			45046.		10/01/0001
Google Cloud	Cloud Tasks		Not Affected		https://cloud.google.	Product		12/21/2021
					com/log4j2-security-	does not		
					advisory	use Log4j		
						2 and is		
						$\operatorname{not}$		
						impacted		
						by the		
						issues		
						identified		
						in		
						CVE-2021-		
						44228 and		
						CVE-2021-		
						45046.		
Google Cloud	Cloud Trace		Not Affected		https://cloud.google.	Product		12/21/2021
Google Cloud	Cloud Trace		Not Affected					12/21/2021
					com/log4j2-security-	does not		
					advisory	use Log4j		
						2 and is		
						not		
						impacted		
						by the		
						issues		
						identified		
						in		
						CVE-2021-		
						44228 and		
						44228 and CVE-2021-		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Cloud Traffic		Not Affected		https://cloud.google.	Product		12/20/2021
	Director				com/log4j2-security-	does not		
					advisory	use $Log4j$		
					v	2 and is		
						not		
						impacted		
						by the		
						issues		
						identified		
						in		
						CVE-2021-		
						44228 and		
						CVE-2021-		
						45046.		
Google Cloud	Cloud		Not Affected		https://cloud.google.	Product		12/21/2021
acogie cioud	Translation		1100 111100004		com/log4j2-security-	does not		12/21/2021
	1141151401011				advisory	use Log4j		
					advisory	use Log4j		
						2 and is		
						not		
						impacted		
						by the		
						issues		
						identified		
						in		
						CVE-2021-		
						44228 and		
						CVE-2021-		
						45046.		
Google Cloud	Cloud VPN		Not Affected		https://cloud.google.	Product		12/20/2021
Google Cloud	Cloud VIIV		Not Affected		11 tops.//cloud.google.			12/20/2021
					com/log4j2-security-	does not		
					advisory	use Log4j		
						2 and is		
						$\operatorname{not}$		
						impacted		
						by the		
						issues		
						identified		
						in		
						CVE-2021-		
						44228  and		
						CVE-2021-		
0 1 0 1	CI 1371 1		NT A CC . 1		1,,, // 1 1 1	45046.		10/01/0001
Google Cloud	Cloud Vision		Not Affected		https://cloud.google.	Product		12/21/2021
					com/log4j2-security-	does not		
					advisory	use $Log4j$		
						2 and is		
						$\operatorname{not}$		
						impacted		
						by the		
						issues		
						identified		
						in		
						CVE-2021-		
						44228 and		
						CVE-2021- 45046.		

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

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

vendor endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Data Catalog		Not Affected		https://cloud.google.	Data		12/20/2021
					com/log4j2-security-	Catalog		
					advisory	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		
						dependen-		
						cies on		
						Log4j 2		
						and		
						update		
						them to		
						the latest		
						version.		

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

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Dataproc		Not Affected		https://cloud.google.	Dataproc		12/20/2021
					com/log4j2-security-	released		
					advisory	new		
						images on		
						December		
						18, 2021 to		
						address		
						the vulner-		
						abilities in		
						CVE-2021-		
						44228 and		
						CVE-2021-		
						45046.		
						Customers		
						$\operatorname{must}$		
						follow the		
						instruc-		
						tions in		
						notifica-		
						tions sent		
						on		
						December		
						18, 2021		
						with the		
						$\operatorname{subject}$		
						line "Im-		
						portant		
						informa-		
						tion about		
						Dataproc"		
						with		
						Dataproc		
						documentat	ion.	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Vendor Google Cloud		Version(s)	Status Not Affected	Update Available	Vendor Link https://cloud.google. com/log4j2-security- advisory	Notes  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 in- structions on December 17, 2021 with the subject line "Im- portant informa- tion regarding Log4j 2 vulnerabil- ity in your		Last Updated 12/20/2021
Google Cloud	Datastore		Not Affected		https://cloud.google. com/log4j2-security- advisory	gRPC- enabled Dataproc Metastore." Product does not use Log4j 2 and is not impacted by the issues identified		12/19/2021
Google Cloud	Datastream		Not Affected		https://cloud.google. com/log4j2-security- advisory	in CVE-2021-44228 and CVE-2021-45046. Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/19/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Dialogflow		Not Affected		https://cloud.google.	Product		12/21/2021
	Essentials (ES)				com/log4j2-security-	does not		
	, ,				advisory	use $Log4j$		
					J. L.	2 and is		
						not		
						impacted		
						by the		
						issues		
						identified		
						in		
						CVE-2021-		
						44228 and		
						CVE-2021-		
						45046.		
Coorle Cloud	Document AI		Not Affected		https://alaud.google	Product		19/91/9091
Google Cloud	Document Ai		Not Affected		https://cloud.google.			12/21/2021
					com/log4j2-security-	does not		
					advisory	use $Log4j$		
						2 and is		
						$\operatorname{not}$		
						impacted		
						by the		
						issues		
						identified		
						in		
						CVE-2021-		
						44228 and		
						CVE-2021-		
						45046.		
Google Cloud	Event Threat		Not Affected		https://cloud.google.	Product		12/21/2021
O	Detection				com/log4j2-security-	does not		, ,
					advisory	use Log4j		
					advisory	2 and is		
						not		
						impacted		
						by the		
						issues		
						identified		
						$_{ m in}$		
						CVE-2021-		
						44228 and		
						CVE-2021-		
G 1 G 1	D		3.T . A.M . 3		1 // 1 1	45046.		10/01/0001
Google Cloud	Eventarc		Not Affected		https://cloud.google.	Product		12/21/2021
					com/log4j2-security-	does not		
					advisory	use $Log4j$		
					-	2 and is		
						not		
						impacted		
						by the		
						issues		
						identified		
						$_{ m in}$		
						CVE-2021-		
						CVE-2021-		
						44228 and CVE-2021-		

ner References	ces Last Updated
ler Keierences	12/21/2021
	12/21/2021
	12/19/2021
	12/21/2021

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

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

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

ndor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
ogle Cloud	Looker		Not Affected		https://cloud.google.	Looker-		12/18/2021
					com/log4j2-security-	hosted		
					advisory	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 vul-		
						nerability.		
						As Looker		
						$\begin{array}{c} \text{does not} \\ \text{enable} \end{array}$		
						logging for		
						these		
						drivers in		
						Looker-		
						hosted		
						instances,		
						no		
						messages		
						are logged.		
					We			
					conclude			
						that the		
						vulnerabil-		
						ity 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 in-		
						structions		
						through		
						their		
						technical		
						contacts		
						on how to		
						take the		
						necessary		
						steps to		
						address		
						the vulner-		
						ability.		
					124	abinty.		
						Looker		
						customers		
						who have		
						questions		
						or require		
						assistance,		
						please visit		
						piease visit		
						Looker		

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

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

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

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

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Speech-to-Text		Not Affected		https://cloud.google.	Product		12/21/2021
					com/log4j2-security-	does not		
					advisory	use Log4j		
					J. 1. 1. 1. 1. J.	2 and is		
						not		
						impacted		
						by the		
						issues		
						identified		
						in		
						CVE-2021-		
						44228 and		
						CVE-2021-		
						45046.		
Coorle Cloud	Speech-to-Text		Not Affected		https://eloud.google	Product		19/91/9091
Google Cloud			Not Affected		https://cloud.google.			12/21/2021
	On-Prem				com/log4j2-security-	does not		
					advisory	use $Log4j$		
						2 and is		
						$\operatorname{not}$		
						impacted		
						by the		
						issues		
						identified		
						in		
						CVE-2021-		
						44228 and		
						CVE-2021-		
						45046.		
Google Cloud	Storage Transfer		Not Affected		https://cloud.google.	Product		12/20/2021
	Service				com/log4j2-security-	does not		, ,
					advisory	use Log4j		
					ddvisory	2 and is		
						not		
						impacted		
						by the		
						issues		
						identified		
						in		
						CVE-2021-		
						44228 and		
						CVE-2021-		
						45046.		
Coorle Claud	Talant Calutian		Not Affected		https://aloud.comla			19 /91 /9091
Google Cloud	Talent Solution		Not Affected		https://cloud.google.	Product		12/21/2021
					com/log4j2-security-	does not		
					advisory	use $Log4j$		
						2 and is		
						$\operatorname{not}$		
						impacted		
						by the		
						issues		
						identified		
						in		
						CVE-2021-		
						44228 and		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	Text-to-Speech		Not Affected		https://cloud.google.	Product		12/21/2021
					com/log4j2-security-	does not		
					advisory	use Log4j		
					v	2 and is		
						not		
						impacted		
						by the		
						issues		
						identified		
						in		
						CVE-2021-		
						44228 and		
						CVE-2021-		
						45046.		
Google Cloud	Transcoder API		Not Affected		https://cloud.google.	Product		12/21/2021
000810 01044	1101100000011111		Trot Illicoted		com/log4j2-security-	does not		12/21/2021
					advisory	use Log4j		
					advisory	use 1.0g4j		
						2 and is		
						not		
						impacted		
						by the		
						issues		
						identified		
						$_{ m in}$		
						CVE-2021-		
						44228 and		
						CVE-2021-		
						45046.		
Google Cloud	Transfor		Not Affected		https://cloud.google.	Product		12/21/2021
Google Cloud			Not Affected		https://cloud.google.			12/21/2021
	Appliance				com/log4j2-security-	does not		
					advisory	use Log4j		
						2 and is		
						$\operatorname{not}$		
						impacted		
						by the		
						issues		
						identified		
						in		
						CVE-2021-		
						44228 and		
						CVE-2021-		
G 1 G 1	371		NT A CC		144 // 1 1 2	45046.		10/01/0001
Google Cloud			Not Affected		https://cloud.google.	Product		12/21/2021
	Intelligence API				com/log4j2-security-	does not		
					advisory	use $Log4j$		
						2 and is		
						not		
						impacted		
						by the		
						issues		
						identified		
						in		
						CVE-2021-		
						44228  and		
						CVE-2021-		

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Gravitee	Access Management	3.10.x	Not Affected	No	About the Log4J CVSS 10 Critical Vulnerability			
Gravitee	Access Management	3.5.x	Not Affected	No	About the Log4J CVSS 10 Critical Vulnerability			
Gravitee	API	3.10.x	Not Affected	No	About the Log4J CVSS			
Gravitee	Management API	3.5.x	Not Affected	No	10 Critical Vulnerability About the Log4J CVSS			
Gravitee	Management Alert Engine	1.5.x	Not Affected	Yes	10 Critical Vulnerability About the Log4J CVSS			
Gravitee	Alert Engine	1.4.x	Not Affected	No	10 Critical Vulnerability About the Log4J CVSS			
Gravitee	Cockpit	1.4.x	Not Affected	No	10 Critical Vulnerability About the Log4J CVSS			
	Соскрп	1.4.X	Not Affected	110	10 Critical Vulnerability			
Gravitee.io Gravwell					Gravitee.io Statement Gravwell Statement			
Graylog	Graylog Server	All versions $>= 1.2.0$ and $<= 4.2.2$	Affected	Yes	Graylog Update for Log4j			
GreenShot Guidewire					GreenShot Statement Guidewire Statement			
HAProxy					HAProxy Statement			
HarmanPro AMX					HarmanPro AMX Statement			
HashiCorp	Boundary		Not Affected		HashiCorp security			
					bulletin re. CVE-2021-44228			
HashiCorp	Consul		Not Affected		HashiCorp security bulletin re.			
IIl-: (C	Comment.		N-+ A (f+-1		CVE-2021-44228			
HashiCorp	Consul Enterprise		Not Affected		HashiCorp security bulletin re.			
HashiCorp	Nomad		Not Affected		CVE-2021-44228 HashiCorp security			
					bulletin re. CVE-2021-44228			
HashiCorp	Nomad		Not Affected		HashiCorp security			
	Enterprise				bulletin re. CVE-2021-44228			
HashiCorp	Packer		Not Affected		HashiCorp security bulletin re.			
TT 1.0			37 . 400 3		CVE-2021-44228			
HashiCorp	Terraform		Not Affected		HashiCorp security bulletin re.			
HashiCorp	Terraform		Not Affected		CVE-2021-44228 HashiCorp security			
rasm corp	Enterprise		1100 111100000		bulletin re.			
HashiCorp	Vagrant		Not Affected		CVE-2021-44228 HashiCorp security			
					bulletin re. CVE-2021-44228			
HashiCorp	Vault		Not Affected		HashiCorp security bulletin re.			
					CVE-2021-44228			
HashiCorp	Vault Enterprise		Not Affected		HashiCorp security bulletin re.			
HashiCorp	Waypoint		Not Affected		CVE-2021-44228 HashiCorp security			
пазіноогр	may point		1100 Milected		bulletin re.			
HCL	BigFix	2.0.1 - 2.0.4	Fixed		CVE-2021-44228 KB with fix	Not	Forum post with more specifics	12/15/2021
Software	Compliance					Affected for related	_	
						CVE-2021-		
						45046		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HCL	BigFix Insights	All	Not Affected		KB	Not		12/15/2021
Software						Affected		
						for related CVE-2021-		
						45046		
HCL Software	BigFix Insights for Vulnerability	All	Not Affected		KB	Not Affected		12/15/2021
DOI: WOLC	Remediation					for related		
						CVE-2021- 45046		
HCL	BigFix	< 10.0.7	Fixed		KB with fix	Not		12/15/2021
Software	Inventory					Affected		
						for related CVE-2021-		
	D. D. T				***	45046		10 (17 (200)
HCL Software	BigFix Lifecycle	All	Not Affected		KB	Not Affected		12/15/2021
Soloware						for related		
						CVE-2021-		
HCL	BigFix Mobile	All	Not Affected		KB	45046 Not		12/15/2021
Software						Affected		
						for related CVE-2021-		
						45046		
HCL Software	BigFix Patch	All	Not Affected		KB	Not Affected		12/15/2021
Software						for related		
						CVE-2021-		
HelpSystems					HelpSystems Clearswift	45046		
Clearswift								
HENIX	Squash TM	1.21.7 - 1.22.9, 2.0.3 - 2.1.5, 2.2.0 - 3.0.2	Fixed		Vendor Link			12/23/2021
Hexagon		2.1.0, 2.2.0 0.0.2			Hexagon Statement			
Hikvision Hitachi	eSOMS		Not Affected		Hikvision Hitachi Energy			
Energy	esoms		Not Affected		Intachi Energy			
Hitachi					Hitachi Vantara			
Vantara Honeywell					Honeywell Statement			
HP	Teradici Cloud	< v113	Fixed	Yes	Apache Log4j update for			2021-12-17
	Access Controller				Teradici PCoIP Connection Manager,			
	Controller				Teradici Cloud Access			
					Connector, Teradici			
					PCoIP License Server, Teradici Management			
					Console, and Teradici			
НР	Teradici	< 1.0.6	Fixed	Yes	EMSDK Apache Log4j update for			2021-12-17
	EMSDK				Teradici PCoIP			
					Connection Manager, Teradici Cloud Access			
					Connector, Teradici			
					PCoIP License Server,			
					Teradici Management Console, and Teradici			
ш	TD 1' '	. 01 10 9	T21 1	V	EMSDK			0001 10 17
HP	Teradici Management	< 21.10.3	Fixed	Yes	Apache Log4j update for Teradici PCoIP			2021-12-17
	Console				Connection Manager,			
					Teradici Cloud Access Connector, Teradici			
					PCoIP License Server,			
					Teradici Management Console, and Teradici			
					EMSDK			

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Vendor	Product Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
HOLOGIC	Unifi Workspace	Affected	No	HOLOGIC Advisory Link	While the Hologic software itself does not utilize Java/Log4J, the installed APC 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	12/20/2021
HOLOGIC	Faxitron CT Specimen Radiography System	Affected	No	HOLOGIC Advisory Link	vulnerable. 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	12/20/2021
HOLOGIC	Dimensions / 3Dimensions Mammography	Not Affected	No	HOLOGIC Advisory Link	program.	12/20/2021
HOLOGIC	System Affirm Prone Biopsy System	Not Affected	No	HOLOGIC Advisory Link		12/20/2021
HOLOGIC	Brevera Breast Biopsy System	Not Affected	No	HOLOGIC Advisory Link		12/20/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
HOLOGIC	Trident HD Specimen Radiography		Not Affected	No	HOLOGIC Advisory Link		12/20/2021
HOLOGIC	System SecurView DX		Not Affected	No	HOLOGIC Advisory		12/20/2021
HOLOGIC	Workstation Cenova Image		Not Affected	No	Link HOLOGIC Advisory		12/20/2021
HOLOGIC	Analytics Server SecurXChange		Not Affected	No	Link HOLOGIC Advisory		12/20/2021
HOLOGIC	Router Rosetta DC Tomosynthesis		Not Affected	No	Link HOLOGIC Advisory Link		12/20/2021
HOLOGIC	Data Converter Faxitron Specimen Radiography Systems		Not Affected	No	HOLOGIC Advisory Link		12/20/2021
HOLOGIC	Horizon DXA Bone		Not Affected	No	HOLOGIC Advisory Link		12/20/2021
HOLOGIC	Densitometer Discovery Bone Densitometer		Not Affected	No	HOLOGIC Advisory Link		12/20/2021
HOLOGIC	Fluoroscan Insight Mini C-Arm		Not Affected	No	HOLOGIC Advisory Link		12/20/2021
HOLOGIC	SuperSonic Imagine Ultrasound Products (Aixplorer & Aixplorer Mach)		Not Affected	No	HOLOGIC Advisory Link		12/20/2021
HOLOGIC	Windows Selenia Mammography System		Not Affected	No	HOLOGIC Advisory Link		12/20/2021
Huawei Hubspot I-Net software I2P IBA-AG Ibexa					Huawei Security Notice Hubspot Notice I-Net Software Statement I2P Statement IBA-AG Statement Ibexa Statement		
IBM	BigFix Compliance		Affected	No	25010 20000110110		
IBM	BigFix Inventory	VM Manager Tool & SAP Tool	Affected	No		To verify if your instance is affected, go to the lib subdi- rectory of the tool (BESClient/LMT/SAPTOOL and BESClient/LMT/VMMAN) and check what version of log4j is included. Version is included in the name of the library.	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	Analytics Engine		Not Affected		An update on the Apache Log4j			12/15/2021
					CVE-2021-44228 vulnerability - IBM PSIRT Blog			
IBM	App		Not Affected		An update on the			12/15/2021
	Configuration				Apache Log4j CVE-2021-44228			
					vulnerability - IBM			
					PSIRT Blog			
$_{\rm IBM}$	App Connect		Not Affected		An update on the			12/15/2021
					Apache Log4j CVE-2021-44228			
					vulnerability - IBM PSIRT Blog			
$_{\mathrm{IBM}}$	App ID		Affected	Yes	An update on the			12/15/2021
					Apache Log4j CVE-2021-44228			
					vulnerability - IBM PSIRT Blog			
$_{\mathrm{IBM}}$	Application		Not Affected		An update on the			12/15/2021
	Gateway				Apache Log4j			, ,
					CVE-2021-44228 vulnerability - IBM			
					PSIRT Blog			
$_{\mathrm{IBM}}$	Aspera		Not Affected		An update on the			12/15/2021
	Endpoint				Apache Log4j CVE-2021-44228			
					vulnerability - $IBM$			
IDM	A		Not Affected		PSIRT Blog			19/15/9091
$_{\mathrm{IBM}}$	Aspera Enterprise		Not Affected		An update on the Apache Log4j			12/15/2021
	•				CVE-2021-44228			
					vulnerability - IBM PSIRT Blog			
$_{\mathrm{IBM}}$	Aspera fasp.io		Not Affected		An update on the			12/15/2021
					Apache Log4j			
					CVE-2021-44228 vulnerability - IBM			
					PSIRT Blog			
$_{\mathrm{IBM}}$	Aspera		Not Affected		An update on the Apache Log4j			12/15/2021
					CVE-2021-44228			
					vulnerability - IBM			
IBM	Bare Metal		Not Affected		PSIRT Blog An update on the			12/15/2021
IDM	Servers		1100 Tiffected		Apache Log4j			12/10/2021
					CVE-2021-44228			
					vulnerability - IBM PSIRT Blog			
$_{\mathrm{IBM}}$	Block Storage		Not Affected		An update on the			12/15/2021
					Apache Log4j CVE-2021-44228			
					vulnerability - IBM			
TD3 -	<b>D</b> 1 • ~				PSIRT Blog			10 /17 /05 -
IBM	Block Storage for VPC		Not Affected		An update on the Apache Log4j			12/15/2021
	101 V1 C				CVE-2021-44228			
					vulnerability - IBM			
IBM	Block Storage		Not Affected		PSIRT Blog An update on the			12/15/2021
11/1/1	Snapshots for		1.00 111100000		Apache Log4j			12/10/2021
	VPC				CVE-2021-44228			
					vulnerability - IBM PSIRT Blog			
					1 DIG DIOS			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	Case Manager		Not Affected		An update on the			 12/15/2021
					Apache Log4j CVE-2021-44228			
					vulnerability - IBM			
					PSIRT Blog			
$_{\mathrm{IBM}}$	Certificate		Affected	Yes	An update on the			12/15/2021
	Manager				Apache Log4j			
					CVE-2021-44228 vulnerability - IBM			
					PSIRT Blog			
$_{\mathrm{IBM}}$	Client VPN for		Not Affected		An update on the			12/15/2021
	VPC				Apache Log4j			
					CVE-2021-44228			
					vulnerability - IBM PSIRT Blog			
$_{\mathrm{IBM}}$	Cloud Activity		Not Affected		An update on the			12/15/2021
	Tracker				Apache Log4j			//
					CVE-2021-44228			
					vulnerability - IBM			
$_{\mathrm{IBM}}$	Cloud Backup		Not Affected		PSIRT Blog An update on the			12/15/2021
IDM	Cloud Dackup		Not Affected		An apaate on the Apache Log4j			12/10/2021
					CVE-2021-44228			
					vulnerability - IBM			
IBM	Cloud		Not Affected		PSIRT Blog An update on the			12/15/2021
IDM	Monitoring		Not Affected		An update on the Apache Log4j			12/13/2021
					CVE-2021-44228			
					vulnerability - $IBM$			
TD3.6			1.00		PSIRT Blog			10/17/0001
$_{\mathrm{IBM}}$	Cloud Object Storage		Affected	Yes	An update on the Apache Log4j			12/15/2021
	Diorage				CVE-2021-44228			
					vulnerability - IBM			
					PSIRT Blog			
$_{\mathrm{IBM}}$	Cloud Object		Affected	Yes	An update on the			12/15/2021
	Storage				Apache Log4j CVE-2021-44228			
					vulnerability - IBM			
					PSIRT Blog			
$_{\mathrm{IBM}}$	Cloudant		Affected	Yes	An update on the			12/15/2021
					Apache Log4j CVE-2021-44228			
					vulnerability - IBM			
					PSIRT Blog			
$_{\mathrm{IBM}}$	Code Engine		Not Affected		An update on the			12/15/2021
					Apache Log4j			
					CVE-2021-44228 vulnerability - IBM			
					PSIRT Blog			
$_{\mathrm{IBM}}$	Cognos		Not Affected		An update on the			12/15/2021
	Command				Apache Log4j			
	Center				CVE-2021-44228			
					vulnerability - IBM PSIRT Blog			
$_{\mathrm{IBM}}$	Cognos	10.4.2	Affected	Yes	Security Bulletin: IBM			12/15/2021
	Controller				Cognos Controller 10.4.2	2		
					IF15: Apache log4j			
					Vulnerability (CVE-2021-44228)			
IBM	Cognos		Not Affected		(CVE-2021-44228) An update on the			12/15/2021
12111	Integration		1.50 111100000		Apache Log4j			//
	Server				CVE-2021-44228			
					vulnerability - IBM			
					PSIRT Blog			

Vendor	Product Version(s	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	Compose Enterprise	Not Affected		An update on the Apache Log4j CVE-2021-44228			12/15/2021
				vulnerability - IBM			
IBM	Compose for	Not Affected		PSIRT Blog An update on the			12/15/2021
IDM	Elasticsearch	Not Affected		An update on the Apache Log4j			12/15/2021
				CVE-2021-44228			
				vulnerability - IBM			
IBM	Compose for	Not Affected		PSIRT Blog An update on the			12/15/2021
IDM	etcd	Not Allected		Apache Log4j			12/10/2021
				CVE-2021-44228			
				vulnerability - IBM			
IBM	Compose for	Not Affected		PSIRT Blog An update on the			12/15/2021
IDM	MongoDB	Not Theeted		Apache Log4j			12/10/2021
				CVE-2021-44228			
				vulnerability - IBM			
IBM	Compose for	Not Affected		PSIRT Blog An update on the			12/15/2021
IDM	MySQL	Not Allected		Apache Log4j			12/10/2021
				CVE-2021-44228			
				vulnerability - IBM			
IBM	Compose for	Not Affected		PSIRT Blog An update on the			12/15/2021
IDM	PostgreSQL	Not Allected		Apache Log4j			12/10/2021
				CVE-2021-44228			
				vulnerability - IBM			
IBM	Compose for	Not Affected		PSIRT Blog An update on the			12/15/2021
IDM	RabbitMQ	Not Affected		An update on the Apache Log4j			12/13/2021
	2000 02012 0			CVE-2021-44228			
				vulnerability - IBM			
IDM	Common for	N - A G - A - 1		PSIRT Blog			19/15/2001
$_{\mathrm{IBM}}$	Compose for Redis	Not Affected		An update on the Apache Log4j			12/15/2021
	Teodis			CVE-2021-44228			
				vulnerability - $IBM$			
IDM	Commons for	Not Affected		PSIRT Blog			19/15/2021
$_{\mathrm{IBM}}$	Compose for RethinkDB	Not Affected		An update on the Apache Log4j			12/15/2021
	Teodimina D			CVE-2021-44228			
				vulnerability - $IBM$			
IDM	Common for	N - A C A - 1		PSIRT Blog			19/15/9001
$_{\mathrm{IBM}}$	Compose for ScyllaDB	Not Affected		An update on the Apache Log4j			12/15/2021
				CVE-2021-44228			
				vulnerability - IBM			
IBM	Containen	Affected	Yes	PSIRT Blog			19/15/2021
IDM	Container Registry	Affected	res	An update on the Apache Log4j			12/15/2021
	regionly			CVE-2021-44228			
				vulnerability - $IBM$			
IDM	Container	A.C 1	Voc	PSIRT Blog			19 /15 /9091
IBM	Container Security	Affected	Yes	An update on the Apache Log4j			12/15/2021
	Services			CVE-2021-44228			
				vulnerability - IBM			
IDM.		3T - 4 00 - 1		PSIRT Blog			10/17/0001
IBM	Content Delivery	Not Affected		An update on the Apache Log4j			12/15/2021
	Network			CVE-2021-44228			
				vulnerability - $IBM$			
				PSIRT Blog			

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	Direct Link Dedicated (2.0)		Not Affected		An update on the Apache Log4j			12/15/2021
					CVE-2021-44228 vulnerability - IBM PSIRT Blog			
IBM	Direct Link		Not Affected		An update on the			12/15/2021
	Dedicated Hosting on				Apache Log4j CVE-2021-44228			7 - 7 -
	Classic				vulnerability - IBM			
	0 20000 2				PSIRT Blog			
$_{\mathrm{IBM}}$	Direct Link		Not Affected		An update on the			12/15/2021
	Dedicated on Classic				Apache Log4j CVE-2021-44228			
	Classic				vulnerability - IBM			
					PSIRT Blog			
IBM	Direct Link		Not Affected		An update on the			12/15/2021
	Exchange on				Apache Log4j			
	Classic				CVE-2021-44228 vulnerability - IBM			
					PSIRT Blog			
IBM	DNS Services		Not Affected		An update on the			12/15/2021
					Apache Log4j			
					CVE-2021-44228			
					vulnerability - IBM PSIRT Blog			
IBM	Emptoris		Not Affected		An update on the			12/15/2021
	Contract				Apache Log4j			, -, -
	Management				CVE-2021-44228			
					vulnerability - IBM			
IBM	Emptoris		Not Affected		PSIRT Blog An update on the			12/15/2021
IDM	Program		Not Thected		Apache Log4j			12/10/2021
	Management				CVE-2021-44228			
					vulnerability - IBM			
IBM	Emptoris		Not Affected		PSIRT Blog An update on the			12/15/2021
IDM	Sourcing		Not Affected		An update on the Apache Log4j			12/10/2021
					CVE-2021-44228			
					vulnerability - IBM			
IDM	Emptonia Spand		Not Affected		PSIRT Blog An update on the			12/15/2021
IBM	Emptoris Spend Analysis		Not Affected		An update on the Apache Log4j			12/13/2021
	Tilloly 515				CVE-2021-44228			
					vulnerability - $IBM$			
TD) f	<b>.</b>		27 . 4		PSIRT Blog			10/17/0001
IBM	Emptoris Supplier		Not Affected		An update on the Apache Log4j			12/15/2021
	Lifecycle				CVE-2021-44228			
	Management				vulnerability - IBM			
					PSIRT Blog			
IBM	Enterprise Tape		Not Affected		An update on the			12/15/2021
	Controller Model C07				Apache Log4j CVE-2021-44228			
	(3592) (ETC)				vulnerability - IBM			
					PSIRT Blog			
IBM	Event		Not Affected		An update on the			12/15/2021
	Notifications				Apache Log4j CVE-2021-44228			
					vulnerability - IBM			
					PSIRT Blog			
IBM	Event Streams		Not Affected		An update on the			12/15/2021
					Apache Log4j			
					CVE-2021-44228 vulnerability - IBM			
					PSIRT Blog			

Vendor	Product Version(s)	Status Update Available	Vendor Link Notes Other References	Last Updated
IBM	File Storage	Not Affected	An update on the	12/15/2021
			Apache Log4j	
			CVE-2021-44228 vulnerability - IBM	
			PSIRT Blog	
IBM	Flash System	Not Affected	An update on the	12/15/2021
	900 (& 840)		Apache Log4j	,,
	,		CVE-2021-44228	
			vulnerability - IBM	
TDM.		N + A (C + 1	PSIRT Blog	10/17/0001
$_{\mathrm{IBM}}$	Flow Logs for VPC	Not Affected	An update on the Apache Log4j	12/15/2021
	VFC		CVE-2021-44228	
			vulnerability - IBM	
			PSIRT Blog	
$_{\mathrm{IBM}}$	Functions	Not Affected	An update on the	12/15/2021
			Apache Log4j	
			CVE-2021-44228	
			vulnerability - IBM PSIRT Blog	
$_{\mathrm{IBM}}$	GSKit	Not Affected	An update on the	12/15/2021
		2.00	Apache Log4j	,,
			CVE-2021-44228	
			vulnerability - IBM	
IDM	G I	N . A	PSIRT Blog	10/17/0001
$_{\mathrm{IBM}}$	Guardium S-TAP for Data	Not Affected	An update on the Apache Log4j	12/15/2021
	Sets on z/OS		CVE-2021-44228	
	5005 011 27 05		vulnerability - IBM	
			PSIRT Blog	
$_{\mathrm{IBM}}$	Guardium	Not Affected	An update on the	12/15/2021
	S-TAP for DB2		Apache Log4j	
	on z/OS		CVE-2021-44228	
			vulnerability - IBM PSIRT Blog	
$_{\mathrm{IBM}}$	Guardium	Not Affected	An update on the	12/15/2021
	S-TAP for IMS		Apache Log4j	, -, -
	on $z/OS$		CVE-2021-44228	
			vulnerability - IBM	
IDM	Haman Duatast	Not Affected	PSIRT Blog	19/15/9091
$_{\rm IBM}$	Hyper Protect Crypto Services	Not Affected	An update on the Apache Log4j	12/15/2021
	Crypto Services		CVE-2021-44228	
			vulnerability - IBM	
			PSIRT Blog	
$_{\mathrm{IBM}}$	Hyper Protect	Affected Yes	An update on the	12/15/2021
	DBaaS for		Apache Log4j	
	MongoDB		CVE-2021-44228 vulnerability - IBM	
			PSIRT Blog	
$_{\mathrm{IBM}}$	Hyper Protect	Affected Yes	An update on the	12/15/2021
	DBaaS for		Apache Log4j	, ,
	PostgreSQL		CVE-2021-44228	
			vulnerability - IBM	
IBM	Hyper Protect	Affected Yes	PSIRT Blog An update on the	12/15/2021
IDM	Virtual Server	Allected 1es	An update on the Apache Log4j	12/10/2021
	Y II UGGI SOL YOL		CVE-2021-44228	
			vulnerability - IBM	
			PSIRT Blog	
IBM	i2 Analyst's	Not Affected	An update on the	12/15/2021
	Notebook		Apache Log4j	
			CVE-2021-44228	
			vulnerability - IBM PSIRT Blog	
			I DILLI DIOR	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	i2 Base		Not Affected		An update on the Apache Log4j			12/15/2021
					CVE-2021-44228			
					vulnerability - IBM			
					PSIRT Blog			
IBM	IBM		Not Affected		An update on the			12/15/2021
	Application				Apache Log4j			
	Runtime Expert				CVE-2021-44228			
	for i				vulnerability - IBM			
TDM.	IDM D 1		NT . A.C 1		PSIRT Blog			10/15/0001
IBM	IBM Backup,		Not Affected		An update on the			12/15/2021
	Recovery and Media Services				Apache Log4j CVE-2021-44228			
	for i				vulnerability - IBM			
	101 1				PSIRT Blog			
IBM	IBM Db2		Not Affected		An update on the			12/15/2021
	Mirror for i				Apache Log4j			, ,
					CVE-2021-44228			
					vulnerability - IBM			
					PSIRT Blog			
IBM	IBM HTTP		Not Affected		An update on the			12/15/2021
	Server				Apache Log4j			
					CVE-2021-44228 vulnerability - IBM			
					PSIRT Blog			
IBM	IBM i Access		Not Affected		An update on the			12/15/2021
12111	Family		1100 111100000		Apache Log4j			12/13/2021
	V				CVE-2021-44228			
					vulnerability - IBM			
					PSIRT Blog			
$_{\mathrm{IBM}}$	IBM i Portfolio		Not Affected		An update on the			12/15/2021
	of products				Apache Log4j			
	under the				CVE-2021-44228			
	Group SWMA				vulnerability - IBM			
IBM	IBM PowerHA		Not Affected		PSIRT Blog An update on the			12/15/2021
IDM	System Mirror		Not Affected		Apache Log4j			12/10/2021
	for i				CVE-2021-44228			
	101 1				vulnerability - IBM			
					PSIRT Blog			
$_{\mathrm{IBM}}$	IBM Sterling		Not Affected		An update on the			12/15/2021
	Connect:Direct				Apache Log4j			
	Browser User				CVE-2021-44228			
	Interface				vulnerability - IBM			
IBM	IBM Sterling	See Vendor Links	Affected	Yes	PSIRT Blog Security Bulletin:		https://www.ibm.com/support/	12/20/2021
IDM	Connect:Direct	See vendor Links	Affected	ies	Apache Log4j		pages/node/6526688,	12/20/2021
	File Agent				Vulnerability Affects		https://www.ibm.com/support/	
	1 110 1180110				IBM Sterling		pages/node/6528324,	
					Connect:Direct for		https://www.ibm.com/blogs/psirt/	
					UNIX		an-update-on-the-apache-log 4 j-cve-	
					(CVE-2021-44228), An		2021-44228-vulnerability/	
					update on the Apache			
IDM	IDM Ctarling		N-4 A.M4-1		Log4j 2.x vulnerabilities	5		19/15/0001
IBM	IBM Sterling Connect:Direct		Not Affected		An update on the Apache Log4j			12/15/2021
	for HP NonStop				CVE-2021-44228			
	101 111 11011010р				vulnerability - IBM			
					PSIRT Blog			
IBM	IBM Sterling		Not Affected		An update on the			12/15/2021
	Connect:Direct				Apache Log4j			
	for $i5/OS$				CVE-2021-44228			
					vulnerability - IBM			
					PSIRT Blog			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	IBM Sterling Connect:Direct		Not Affected		An update on the Apache Log4j			12/15/2021
	for OpenVMS				CVE-2021-44228 vulnerability - IBM			
					PSIRT Blog			
IBM	IBM Sterling Con-		Not Affected		An update on the Apache Log4j			12/15/2021
	nect:Express for				CVE-2021-44228			
	Microsoft				vulnerability - $IBM$			
TD1.	Windows		37 . 100 . 1		PSIRT Blog			10/17/10001
IBM	IBM Sterling Con-		Not Affected		An update on the Apache Log4j			12/15/2021
	nect:Express for				CVE-2021-44228			
	UNIX				vulnerability - IBM			
IBM	IBM Sterling		Not Affected		PSIRT Blog An update on the			12/15/2021
IDM	Con-		Not Affected		An update on the Apache Log4j			12/13/2021
	nect:Express for				CVE-2021-44228			
	z/OS				vulnerability - IBM			
IBM	Instana Agent	Timestamp lower than	Affected	Yes	PSIRT Blog Status Instana			12/14/2021
	Instana Agent	12-11-2021						
IBM	Internet Services		Affected	Yes	An update on the Apache Log4j			12/15/2021
	DOI VICOS				CVE-2021-44228			
					vulnerability - $IBM$			
TDM (	T/ T:0 1		NT + A CC + 1		PSIRT Blog			10/15/2001
IBM	Key Lifecyle Manager for		Not Affected		An update on the Apache Log4j			12/15/2021
	z/OS				CVE-2021-44228			
	2/05				vulnerability - $IBM$			
TDM (	IZ D		NI ACC		PSIRT Blog			10/15/2001
IBM	Key Protect		Not Affected		An update on the Apache Log4j			12/15/2021
					CVE-2021-44228			
					vulnerability - $IBM$			
IBM	Knowledge		Affected	Yes	PSIRT Blog An update on the			12/15/2021
IDM	Studio		Affected	ies	An update on the Apache Log4j			12/13/2021
					CVE-2021-44228			
					vulnerability - IBM			
IBM	Kubernetes		Not Affected		PSIRT Blog An update on the			12/15/2021
IDM	Service		Not Affected		An update on the Apache Log4j			12/13/2021
					CVE-2021-44228			
					vulnerability - IBM			
IBM	Load Balancer		Not Affected		PSIRT Blog An update on the			12/15/2021
111/1/1	for VPC		Not Allected		An update on the Apache Log4j			12/10/2021
					CVE-2021-44228			
					vulnerability - IBM			
IBM	Log Analysis		Not Affected		PSIRT Blog An update on the			12/15/2021
	208 Timoryon		1.00 Illicolou		Apache Log4j			12/10/2021
					CVE-2021-44228			
					vulnerability - IBM			
IBM	Managed		Affected	Yes	PSIRT Blog An update on the			12/15/2021
	VMware Service		111100000		Apache Log4j			12/10/2021
					CVE-2021-44228			
					vulnerability - IBM			
IBM	Management		Affected	No	PSIRT Blog			
1171/1	Extender for		meeted	110				
	VMware							
	vCenter							

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	Mass Data		Not Affected		An update on the			12/15/2021
	Migration				Apache Log4j			
					CVE-2021-44228			
					vulnerability - IBM			
IBM	Maximo EAM		Not Affected		PSIRT Blog An update on the			12/15/2021
IDM	SaaS		Not Affected		An update on the Apache Log4j			12/13/2021
	Saas				CVE-2021-44228			
					vulnerability - IBM			
					PSIRT Blog			
IBM	Message Hub		Not Affected		An update on the			12/15/2021
					Apache Log4j			
					CVE-2021-44228			
					vulnerability - IBM			
					PSIRT Blog			
IBM	MQ Appliance		Not Affected		An update on the			12/15/2021
					Apache Log4j			
					CVE-2021-44228			
					vulnerability - IBM			
IBM	MQ on IBM		Not Affected		PSIRT Blog An update on the			12/15/2021
IDM	Cloud		Not Affected		An update on the Apache Log4j			12/13/2021
	Cloud				CVE-2021-44228			
					vulnerability - IBM			
					PSIRT Blog			
IBM	Natural		Affected	Yes	An update on the			12/15/2021
	Language				Apache Log4j			7 -7 -
	Understanding				CVE-2021-44228			
					vulnerability - IBM			
					PSIRT Blog			
$_{\mathrm{IBM}}$	OmniFind Text		Not Affected		An update on the			12/15/2021
	Search Server				Apache Log4j			
	for DB2 for i				CVE-2021-44228			
					vulnerability - IBM			
IDM	ODENDMO		NI-+ Aff+-1		PSIRT Blog			19/17/2021
IBM	OPENBMC		Not Affected		An update on the			12/15/2021
					Apache Log4j CVE-2021-44228			
					vulnerability - IBM			
					PSIRT Blog			
$_{\mathrm{IBM}}$	Planning	> 2.0.57	Affected	Yes	Security Bulletin: IBM			12/15/2021
	Analytics				Planning Analytics 2.0:			
	Workspace				Apache log4j			
					Vulnerability			
					(CVE-2021-44228)			
$_{\rm IBM}$	Power HMC	V9.2.950.0 &	Affected	Yes	Security Bulletin:			12/15/2021
		V10.1.1010.0			Vulnerability in Apache			
					Log4j (CVE-2021-44228)			
IDM	DCC		NI-+ AC+-1		affects Power HMC			19/17/2021
IBM	PowerSC		Not Affected		An update on the			12/15/2021
					Apache Log4j CVE-2021-44228			
					vulnerability - IBM			
					PSIRT Blog			
IBM	PowerVM		Not Affected		An update on the			12/15/2021
	Hypervisor				Apache Log4j			//
	V I				CVE-2021-44228			
					vulnerability - IBM			
					PSIRT Blog			
IBM	PowerVM VIOS		Not Affected		An update on the			12/15/2021
					Apache Log4j			
					CVE-2021-44228			
					vulnerability - IBM PSIRT Blog			

Vendor	Product Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
BM	QRadar Advisor	Not Affected		An update on the			12/15/2021
				Apache Log4j			
				CVE-2021-44228			
				vulnerability - $IBM$			
				PSIRT Blog			
M	Qradar Network	Not Affected		An update on the			12/15/2021
	Threat			Apache Log4j			
	Analytics			CVE-2021-44228			
				vulnerability - IBM			
				PSIRT Blog			
M	QRadar SIEM	Not Affected		An update on the			12/15/2021
				Apache Log4j			
				CVE-2021-44228			
				vulnerability - IBM			
				PSIRT Blog			
M	Quantum	Not Affected		An update on the			12/15/2021
	Services			Apache Log4j			
				CVE-2021-44228			
				vulnerability - IBM			
				PSIRT Blog			
M	Rational	Not Affected		An update on the			12/15/2021
	Developer for			Apache Log4j			• •
	AIX and Linux			CVE-2021-44228			
				vulnerability - IBM			
				PSIRT Blog			
M	Rational	Not Affected		An update on the			12/15/2021
	Developer for i			Apache Log4j			, ,
	•			CVE-2021-44228			
				vulnerability - IBM			
				PSIRT Blog			
M	Red Hat	Not Affected		An update on the			12/15/2021
	OpenShift on			Apache Log4j			//
	IBM Cloud			CVE-2021-44228			
	2211 01044			vulnerability - IBM			
				PSIRT Blog			
M	Resilient	Under		1 22102 2308			
		Investigation					
M	Robotic Process	Not Affected		An update on the			12/15/2021
	Automation	1.00 11110000		Apache Log4j			12/13/2011
	11000110011001			CVE-2021-44228			
				vulnerability - IBM			
				PSIRT Blog			
$^{\mathrm{SM}}$	SAN Volume	Not Affected		An update on the			12/15/2021
	Controller and	1100 IIIIcooca		Apache Log4j			12/10/2021
	Storwize Family			CVE-2021-44228			
	Storwize ranning			vulnerability - IBM			
				PSIRT Blog			
M	Satellite	Not Affected		An update on the			12/15/2021
IVI	Infrastructure	Not Affected		An update on the Apache Log4j			12/13/2021
	Service			CVE-2021-44228			
	Service			vulnerability - IBM			
				PSIRT Blog			
M	Calcanation	Not Affected		9			19/15/9091
M	Schematics	Not Affected		An update on the			12/15/2021
				Apache Log4j			
				CVE-2021-44228			
				vulnerability - IBM			
M.	Canada Mara	M-+ AC + 1		PSIRT Blog			10/15/0001
M	Secrets Manager	Not Affected		An update on the			12/15/2021
				Apache Log4j			
				CVE-2021-44228			
				vulnerability - IBM			
				PSIRT Blog			
M	Secure Gateway	Not Affected		An update on the			12/15/2021
				Apache Log4j			
				CVE-2021-44228			
				vulnerability - IBM			
				PSIRT Blog			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	Server Automation		Affected	No				
BM	Spectrum		Not Affected		An update on the			12/15/2021
	Archive Library				Apache Log4j			, ,
	Edition				CVE-2021-44228			
					vulnerability - IBM			
			37		PSIRT Blog			10/17/0001
BM	Spectrum		Not Affected		An update on the			12/15/2021
	Discover				Apache Log4j CVE-2021-44228			
					vulnerability - IBM			
					PSIRT Blog			
ВМ	Spectrum		Not Affected		An update on the			12/15/2021
	Protect Client				Apache Log4j			, ,
	Management				CVE-2021-44228			
	Service				vulnerability - IBM			
	_				PSIRT Blog			
BM	Spectrum		Not Affected		An update on the			12/15/2021
	Protect for Databases:				Apache Log4j			
	Databases: Data Protection				CVE-2021-44228 vulnerability - IBM			
	for Oracle				PSIRT Blog			
BM	Spectrum		Not Affected		An update on the			12/15/2021
	Protect for		1.00 111100000		Apache Log4j			12/10/2021
	Databases:				CVE-2021-44228			
	Data Protection				vulnerability - IBM			
	for SQL				PSIRT Blog			
$_{\mathrm{BM}}$	Spectrum		Not Affected		An update on the			12/15/2021
	Protect for				Apache Log4j			
	Enterprise Resource				CVE-2021-44228 vulnerability - IBM			
	Planning				PSIRT Blog			
ВМ	Spectrum		Not Affected		An update on the			12/15/2021
5111	Protect for Mail:		1100 IIIIccocc		Apache Log4j			12/10/2021
	Data Protection				CVE-2021-44228			
	for Domino				vulnerability - IBM			
					PSIRT Blog			
$_{ m BM}$	Spectrum		Not Affected		An update on the			12/15/2021
	Protect for Mail:				Apache Log4j			
	Data Protection				CVE-2021-44228			
	for Exchange				vulnerability - IBM PSIRT Blog			
BM	Spectrum		Not Affected		An update on the			12/15/2021
JM	Protect for		1100 Hilledea		Apache Log4j			12/19/2021
	Workstations				CVE-2021-44228			
					vulnerability - IBM			
					PSIRT Blog			
BM	Spectrum		Not Affected		An update on the			12/15/2021
	Protect for				Apache Log4j			
	z/OS USS				CVE-2021-44228			
	Client and API				vulnerability - IBM			
BM	Spectrum		Not Affected		PSIRT Blog An update on the			12/15/2021
DIM	Protect Plus		Not Allected		An update on the Apache Log4j			12/10/2021
	Db2 Agent				CVE-2021-44228			
	2 - 2 1180110				vulnerability - IBM			
					PSIRT Blog			
ВМ	Spectrum		Not Affected		An update on the			12/15/2021
	Protect Plus				Apache Log4j			
	Exchange Agent				CVE-2021-44228			
					vulnerability - IBM			
D) f	G ·		37 . 100		PSIRT Blog			10/12/1000
BM	Spectrum		Not Affected		An update on the			12/15/2021
	Protect Plus				Apache Log4j			
	File Systems Agent				CVE-2021-44228 vulnerability - IBM			
	лдени				PSIRT Blog			
					PSIRT Rlog			

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	 Last Updated
IBM	Tape System Library Manager		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM			12/15/2021
IBM	TDMF for zOS		Not Affected		PSIRT Blog An update on the Apache Log4j CVE-2021-44228			12/15/2021
IBM	Total Storage Service Console		Not Affected		vulnerability - IBM PSIRT Blog An update on the Apache Log4j			12/15/2021
IDM.	(TSSC) / TS4500 IMC		N + AC + 1		CVE-2021-44228 vulnerability - IBM PSIRT Blog			10 /17 /0001
IBM	Transit Gateway		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM			12/15/2021
IBM	Tririga Anywhere		Not Affected		PSIRT Blog An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM			12/15/2021
IBM	TS4300		Not Affected		PSIRT Blog An update on the Apache Log4j CVE-2021-44228			12/15/2021
IBM	Urbancode Deploy		Not Affected		vulnerability - IBM PSIRT Blog An update on the Apache Log4j CVE-2021-44228			12/15/2021
IBM	Virtual Private Cloud		Not Affected		vulnerability - IBM PSIRT Blog An update on the Apache Log4j CVE-2021-44228			12/15/2021
IBM	Virtual Server for Classic		Not Affected		vulnerability - IBM PSIRT Blog An update on the Apache Log4j CVE-2021-44228			12/15/2021
IBM	Virtualization Management Interface		Not Affected		vulnerability - IBM PSIRT Blog An update on the Apache Log4j CVE-2021-44228			12/15/2021
IBM	VMware Solutions		Affected	Yes	vulnerability - IBM PSIRT Blog An update on the Apache Log4j CVE-2021-44228			12/15/2021
IBM	VMware vCenter Server		Affected	Yes	vulnerability - IBM PSIRT Blog An update on the Apache Log4j CVE-2021-44228			12/15/2021
IBM	VMware vSphere		Affected	Yes	vulnerability - IBM PSIRT Blog An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
BM	VPN for VPC		Not Affected		An update on the			12/15/2021
					Apache Log4j			
					CVE-2021-44228			
					vulnerability - IBM			
ВМ	vRealize		A (C + - 1	<b>V</b>	PSIRT Blog			19/15/9091
DM	Operations and		Affected	Yes	An update on the Apache Log4j			12/15/2021
	Log Insight				CVE-2021-44228			
	Log msignt				vulnerability - IBM			
					PSIRT Blog			
BM	Workload		Not Affected		An update on the			12/15/2021
2	Automation		1100 111100000		Apache Log4j			12/10/2021
					CVE-2021-44228			
					vulnerability - IBM			
					PSIRT Blog			
CONICS	All		Not Affected		ICONICS Advisory Link			12/21/2021
FS					IFS Bulletin			
$\operatorname{GEL}$					IGEL Statement			
gnite					Ignite Realtime			
Realtime					Statement			
iGrafx					iGrafx Statement			
Illuminated					Illuminated Cloud			
Cloud	G TITAL		27 . 1		Statement			10/10/0001
Illumio	C-VEN		Not Affected		Illumio KB article			12/16/2021
Illumio	CLI		Not Affected		Illumio KB article			12/16/2021
Illumio	CloudSecure		Not Affected		Illumio KB article			12/16/2021
Illumio	Core on-premise PCE		Not Affected		Illumio KB article			12/16/2021
Illumio	Core SaaS PCE		Not Affected		Illumio KB article			12/16/2021
Illumio	Edge SaaS PCE		Not Affected		Illumio KB article			$\frac{12/16/2021}{12/16/2021}$
Illumio	Edge Saas 1 CE Edge-		Not Affected		Illumio KB article			$\frac{12}{10},\frac{10}{2021}$
mamo	CrowdStrike		1100 Tineeded		mumo RD article			12/10/2021
Illumio	Flowlink		Not Affected		Illumio KB article			12/16/2021
Illumio	Kubelink		Not Affected		Illumio KB article			12/16/2021
Illumio	NEN		Not Affected		Illumio KB article			12/16/2021
Illumio	QRadar App		Not Affected		Illumio KB article			12/16/2021
Illumio	Splunk App		Not Affected		Illumio KB article			12/16/2021
Illumio	VEN		Not Affected		Illumio KB article			12/16/2021
IManage					IManage Statement			
Imperva					Imperva Statement			
Inductive					Inductive Automation			
Automation					Statement			
IndustrialDef	fender				IndustrialDefender			
					Statement			
infinidat					infinidat Statement InfluxData Statement			
InfluxData Infoblox					Infoblox Statement			
Informatica					Informatica Statement			
Instana					Instana Statement			
Instructure					Instructure Statement			
Intel	Audio		Affected	No	Intel Advisory			12/16/2021
	Development				J			
	Kit							
intel	Datacenter		Affected	No	Intel Advisory			12/16/2021
	Manager				·			
Intel	oneAPI sample		Affected		Intel Advisory			12/16/2021
	browser plugin							
	for Eclipse							
Intel	System		Affected		Intel Advisory			12/16/2021
	Debugger							
Intel	Secure Device		Affected		Intel Advisory			12/16/2021
r , 1	Onboard		A (C)		T / 1 4 1 ·			10 /10 /0001
Intel	Genomics		Affected		Intel Advisory			12/16/2021
Intol	Kernel Library		A ffoot - J		Intol Advisor-			19/16/9001
Intel	System Studio		Affected		Intel Advisory			12/16/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Intel	Computer Vision Annotation Tool maintained by Intel		Affected		Intel Advisory		12/16/2021
Intel	Sensor Solution Firmware Development Kit		Affected		Intel Advisory		12/16/2021
Internet Systems Consortium(IS	ISC DHCP, aka dhcpd	All	Not Affected	N/A	ISC Open Source and Log4J	no JAVA Code	12/17/2021
Internet Systems Consortium(IS	Kea DHCP	All	Not Affected	N/A	ISC Open Source and $Log 4J$	no JAVA Code	12/17/2021
Internet Systems Consortium(IS	BIND 9	All	Not Affected	N/A	ISC Open Source and $Log 4J$	no JAVA Code	12/17/2021
InterSystems Intland	codebeamer	<= 20.11-SP11, <= 21.09-SP3	Affected	Some releases	InterSystems Statement Apache Log4j vulnerability and fixes	A fix has been released for 20.11 and 21.09, but not yet for 21.04	
IPRO iRedMail Ironnet  ISLONLINE Ivanti Jamasoftware	Netgovern				iRedMail Statement Ironnet Security Notification ISLONLINE Statement Ivanti Statement Jamasoftware Statement		
Jamf Jaspersoft Jedox	Jamf Pro	10.31.0 - 10.34.0	Affected	Yes	Mitigating the Apache Log4j 2 Vulnerability Jaspersoft Statement Jedox Statement		
Jenkins Jenkins	CI/CD Core Plugins		Not Affected Some affected, some fixed, most unaffected. See issue tracker	Some	Announcement, issue tracker	Instructions to test your instal- lations in announce- ment	2021-12-16
JetBrains	IntelliJ platform based IDEs (AppCode, CLion, DataGrip, DataSpell, GoLand, IntelliJ IDEA Ulti- mate/Community PhpStorm, PyCharm Profes- sional/Communit Rider, RubyMine, WebStorm)	r/Edu,	Not Affected		JetBrains Blog Post		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
etBrains	All .NET tools (ReSharper, Rider, ReSharper C++, dotTrace, dotMemory, dotCover, dotPeek)	Unknown	Not Affected		JetBrains Blog Post			
JetBrains 1	ToolBox	Unknown	Not Affected		JetBrains Blog Post			
letBrains	TeamCity	Unknown	Not Affected		JetBrains Blog Post			
letBrains	Hub	2021.1.14080	Fixed		JetBrains Blog Post			
etBrains	YouTrack Standalone	2021.4.35970	Fixed		JetBrains Blog Post			
letBrains	YouTrack InCloud	Unknown	Fixed		JetBrains Blog Post			
${ m JetBrains}$	Datalore	Unknown	Not Affected		JetBrains Blog Post			
${ m JetBrains}$	Space	Unknown	Not Affected		JetBrains Blog Post			
Jetbrains	Code With Me	Unknown	Fixed		JetBrains Blog Post			
$\operatorname{JetBrains}$	Gateway	Unknown	Not Affected		JetBrains Blog Post			
JetBrains	Kotlin	Unknown	Not Affected		JetBrains Blog Post			
${ m JetBrains}$	Ktor	Unknown	Not Affected		JetBrains Blog Post			
JetBrains	MPS	Unknown	Not Affected		JetBrains Blog Post			
JetBrains	Floating license server	30211	Fixed		JetBrains Blog Post			
$\operatorname{JetBrains}$	UpSource	2020.1.1952	Fixed		JetBrains Blog Post			
JFROG					JFROG Statement			
Jitsi					Jitsi Advisory			
itterbit					Jitterbit Statement			
POS	(ISO-8583) bridge	Unknown	Not Affected		source			
ohnson Controls	C • CURE-9000	2.90.x (all 2.90 versions)	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	C • CURE-9000	2.80.x (all 2.80 versions)	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls	C • CURE-9000	2.70 (All versions)	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls Johnson	C • CURE-9000	2.60 (All versions) 5.x	Not Affected Not Affected		Johnson Controls Advisory Link Johnson Controls			12/21/2021 $12/21/2021$
Controls Johnson	victor victor/	3.81.x / victor 5.4.1 /	Not Affected		Advisory Link Johnson Controls			12/21/2021
Controls	C • CURE-9000 Unified	C • CURE-9000 2.80	Tiou Tineouou		Advisory Link			12/21/2021
Johnson	victor/	3.91.x / victor 5.6.1 /	Not Affected		Johnson Controls			12/21/2021
Controls	C • CURE-9000 Unified	C • CURE-9000 2.90			Advisory Link			, ,
Johnson	Metasys	All versions	Not Affected		Johnson Controls			12/21/2021
Controls	Products and Tools				Advisory Link			
ohnson Controls	Facility Explorer	14.x	Not Affected		Johnson Controls Advisory Link			12/21/2021
Johnson Controls Johnson	CEM AC2000 CEM Hardware	All versions  All versions	Not Affected Not Affected		Johnson Controls Advisory Link Johnson Controls			12/21/2021 $12/21/2021$
Controls Johnson	Products Illustra Cameras	All versions	Not Affected		Advisory Link Johnson Controls			12/21/2021
Controls Johnson	Illustra Insight	All versions	Not Affected		Advisory Link Johnson Controls			12/21/2021
Controls Johnson	Tyco AI	All versions	Not Affected		Advisory Link Johnson Controls			12/21/2021
Controls Johnson	DLS	All versions	Not Affected		Advisory Link Johnson Controls			12/21/2021
Controls Johnson Controls	Entrapass	All versions	Not Affected		Advisory Link Johnson Controls Advisory Link			12/21/2021
Controls Johnson Controls	CloudVue Web	All versions	Not Affected		Advisory Link Johnson Controls Advisory Link			12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
hnson	CloudVue	All versions	Not Affected		Johnson Controls			12/21/2021
ntrols	Gateway				Advisory Link			
nnson	Qolsys IQ	All versions	Not Affected		Johnson Controls			12/21/2021
ntrols	Panels		37 . 100 . 1		Advisory Link			10/01/0001
nnson	PowerSeries	All versions	Not Affected		Johnson Controls			12/21/2021
ntrols	NEO	A 11 ·	NI A C A 1		Advisory Link			10 /01 /0001
nnson	PowerSeries Pro	All versions	Not Affected		Johnson Controls			12/21/2021
ontrols hnson	Sur-Gard	All versions	Not Affected		Advisory Link Johnson Controls			19/91/9091
ontrols	Receivers	All versions	Not Affected		Advisory Link			12/21/2021
hnson	VideoEdge	5.x	Not Affected		Johnson Controls			12/21/2021
ontrols	VideoEdge	5.X	Not Affected		Advisory Link			12/21/2021
hnson	exacqVision	All versions	Not Affected		Johnson Controls			12/21/2021
ontrols	Server	TIII VOIDIOIID	1100 111100000		Advisory Link			12/21/2021
hnson	exacqVision	All versions	Not Affected		Johnson Controls			12/21/2021
ontrols	Client				Advisory Link			, ,
hnson	exacqVision	All versions	Not Affected		Johnson Controls			12/21/2021
ntrols	WebService				Advisory Link			, ,
nnson	BCPro	All versions	Not Affected		Johnson Controls			12/21/2021
ntrols					Advisory Link			
nnson	iSTAR	All versions	Not Affected		Johnson Controls			12/21/2021
ontrols					Advisory Link			
urnyx					Journeyx Statement			
mp					Jump Desktop			
esktop					Statement			
niper					Juniper Networks			
etworks					Statement			
stice					Justice Systems Support	t		
stems					TZ1F1 Cl			
5t					K15t Statement			
3 arakun					K6 Statement Karakun Statement			
arakun aseya					Karakun Statement Kaseya Vulnerability			
aseya					Assessment			
eeper					Keeper Security Notice			
curity					Reeper Security Notice			
EMP					KEMP Support			
EMP 2					KEMP 2 Support			
ofax					Kofax Product			
01011					Information			
onica					Konica Minolta Support	t		
inolta								
ronos UKG					Kronos UKG Statement	;		
yberna					Kyberna Statement			
Soft					L-Soft Info			
Harris					L3Harris Geospatial			
ospatial								
ncom					Lancom Systems			
stems					General Security			
					Information			
nsweeper					Lansweeper Information	l		
serfiche					Laserfiche Product			
-4D					Information			
stPass					LastPass Information			
unchDarkly					LaunchDarkly			
oniz					Statement Leanix Statement			
anix ica	Aperio AT2		Not Affected		Leanix Statement Leica BIOSYSTEMS			12/21/2021
ica OSYSTEM			Not Affected		Advisory Link			12/21/2021
ica	Aperio AT2 DX		Not Affected		Leica BIOSYSTEMS			12/21/2021
osystem			Not Affected		Advisory Link			12/21/2021
ica	Aperio CS2		Not Affected		Leica BIOSYSTEMS			12/21/2021
OSYSTEM			1100 IIIIecteu		Advisory Link			12/21/2021
ica	Aperio eSlide		Not Affected		Leica BIOSYSTEMS			12/21/2021
			1100 Miletted		Advisory Link			12/21/2021
	S Manager				AUVISOLVIJIIK			
osystem ica	S Manager Aperio GT 450		Not Affected		Leica BIOSYSTEMS			12/21/2021

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

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Lenovo	XClarity Mobile		Not Affected		Apache Log4j			2021-12-14
Lenovo	(LXCM) XClarity Orchestrator		Not Affected		Vulnerability Apache Log4j Vulnerability			2021-12-14
Lenovo	(LXCO) XClarity Provisioning Manager		Not Affected		Apache Log4j Vulnerability			2021-12-14
LeoStream Let's Encrypt LibreNMS LifeRay LifeSize Lightbend Lime CRM LIONGARD LiquidFiles LiveAction Loftware	(LXPM)				LeoStream Discussion Let's Enrypt Statement LibreNMS Statement LifeRay Blog LifeSize Statement Lightbend Statement Lime CRM Statement LIONGARD FAQ LiquidFiles Statement LiveAction Statement Loftware			
LOGalyze	SIEM & log analyzer tool	v4.x	Affected	No	abandoned open-source software repo (sourceforge.net)	local-log4j-vuln-scanner result: indicator for vulnerable component found in /logalyze/lib. 1.2.17.jar (org/apache/log4j 1.2.17	Forks (github.com) //log4j- //log4j/net/SocketNode.class):	2021-12-17
LogiAnalytics LogicMonitor	LogicMonitor Platform		Not Affected		LogiAnalytics Statement Log4j Security Vulnerabilities LogMeIn Statement	1.2.11		
LogRhythm Looker	Looker	21.0, 21.6, 21.12, 21.16, 21.18, 21.20	Affected	Yes	LogRhythm Statement Looker Statement			
LucaNet Lucee Lyrasis	Fedora Repository	3.x,4.x,5.x,6.x	Not Affected		LucaNet Statement Lucee Statement Fedora Repository Statement	Fedora Repository is unaffili- ated with Fedora Linux. Uses logback and explicitly excludes		2021-12-14
MailStore Maltego					MailStore Statement Maltego Response to Logj4	log4j.		
ManageEngine	Servicedesk Plus	11305 and below	Affected		Manage Engine Advisory			12/15/2021
ManageEngine	AD SelfService Plus	Build 6.1 build 6114	Not Affected		1 KUVISOI Y		12/27/21	
ManageEngine Zoho					Manage Engine Link			
ManageEngine Zoho	ADManager Plus	On-Prem			ManageEngine Vulnerability Impact			12/16/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
ManageEngine Zoho	ADAudit Plus	On-Prem			ManageEngine Vulnerability Impact			12/16/2021
ManageEngine		On-Prem			ManageEngine			12/16/2021
Zoho ManageEngine	Plus EventLog	On-Prem			Vulnerability Impact ManageEngine			12/16/2021
Zoho	Analyzer				Vulnerability Impact			
ManageEngine Zoho	M365 Manager Plus	On-Prem			ManageEngine Vulnerability Impact			12/16/2021
ManageEngine Zoho	RecoveryManager Plus	On-Prem			ManageEngine Vulnerability Impact			12/16/2021
ManageEngine	Exchange	On-Prem			ManageEngine			12/16/2021
Zoho ManageEngine	Reporter Plus Log360	On-Prem			Vulnerability Impact ManageEngine			12/16/2021
Zoho					Vulnerability Impact			
ManageEngine Zoho	Log360 UEBA	On-Prem			ManageEngine Vulnerability Impact			12/16/2021
ManageEngine Zoho	Cloud Security Plus	On-Prem			ManageEngine Vulnerability Impact			12/16/2021
ManageEngine	M365 Security	On-Prem			ManageEngine			12/16/2021
Zoho ManageEngine	Plus Analytics Plus	On-Prem			Vulnerability Impact ManageEngine			12/16/2021
Zoho MariaDB	· ·				Vulnerability Impact MariaDB Statement			, ,
MathWorks	All MathWorks		Not Affected	No	MathWorks statement			
	general release desktop or				regarding CVE-2021-44228			
3.6 -1377 1	server products							
MathWorks Matlab					MathWorks Matlab Statement			
Matillion					Matillion Security Advisory			
Matomo					Matomo Statement			
Mattermost FocalBoard					Mattermost FocalBoard Concern			
McAfee	Data Exchange		Not Affected		0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0			12/20/2021
	Layer (DXL) Client							
McAfee	Data Loss Prevention		Not Affected					12/20/2021
	(DLP) Discover							
McAfee	Data Loss Prevention		Not Affected					12/20/2021
	(DLP) Endpoint							
McAfee	for Mac Data Loss		Not Affected					12/20/2021
	Prevention (DLP) Endpoint							
35.40	for Windows		37 . 100 . 1					10/00/0004
McAfee	Data Loss Prevention		Not Affected					12/20/2021
MaAfaa	(DLP) Monitor		Not Affected					19 /90 /9091
McAfee	Data Loss Prevention		Not Affected					12/20/2021
McAfee	(DLP) Prevent Endpoint		Not Affected					12/20/2021
Wichice	Security (ENS)		1100 Hitched					12/20/2021
McAfee	for Linux Endpoint		Not Affected					12/20/2021
	Security (ENS)							, ,
McAfee	for Mac Endpoint		Not Affected					12/20/2021
	Security (ENS) for Windows							
McAfee	ePolicy	5.10 CU11	Fixed	Yes	https://kc.mcafee.com/			12/20/2021
	Orchestrator Application				agent/index?page= content&id=SB10377			
	Server (ePO)							

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
MEINBERG					MEINBERG			
					Information			
Meltano	Meltano		Not affected		Meltano	Project is		
						written in		
						Python		
Memurai					Memurai Information	- J		
MicroFocus					MicroFocus Statement			
Microsoft	Azure		Not Affected		Microsoft's Response t	n		
VIIC105010	Application		1100 Tinecoca		CVE-2021-44228 Apach			
	Gateway				Log4j 2	ic		
Microsoft	Azure API		Not Affected		Microsoft's Response t	0		
WICIOSOIT	Gateway		Not Affected		CVE-2021-44228 Apach			
	Gateway					ie		
N 1: C+	A D-4- 1-1	< 0.2.10	A.C 4 - 1		Log4j 2			
Microsoft	Azure Data lake	< 2.3.10	Affected		azure-data-lake-store-			
	store java				java/CHANGES.md at		. 140	
					ed5d6304783286c3cfff0a	11dee457a922e2	3ad48	
					· Azure/azure-data-			
					lake-store-java			
					GitHub			
Microsoft	Azure Data lake	< 2.3.10	Affected		azure-data-lake-store-			
	store java				java/CHANGES.md at			
					ed5d6304783286c3cfff0a	1 dee 457 a 922 e 2	3ad48	
					· Azure/azure-data-			
					lake-store-java ·			
					$\operatorname{GitHub}$			
Microsoft	Azure DevOps	2019.0 - 2020.1	Affected	No	Azure DevOps (and			
	Server				Azure DevOps Server)			
					and the log4j			
					vulnerability			
Microsoft	Azure DevOps		Not Affected		Azure DevOps (and			
					Azure DevOps Server)			
					and the log4j			
					vulnerability			
Microsoft	Azure Traffic		Not Affected		Microsoft's Response t	0		
	Manager		1100 111100000		CVE-2021-44228 Apach			
	Manager				Log4j 2			
Microsoft	Team	2018.2+	Affected	No	Azure DevOps (and			
VIICIOSOIT	Foundation	2010.27	Allected	110	Azure DevOps (and Azure DevOps Server)			
	Server				and the log4j			
	Server				vulnerability			
Microstrategy						.+		
Midori					Microstrategy Statemer Midori Global	10		
Global					Statement			
Mikrotik					Mikrotik Statement			
Milestone sys					Milestone sys Statemen	nt		
Mimecast					Mimecast Information			
Minecraft					Minecraft Vulnerability	7		
					Message			
Mirantis					Mirantis Statement			
Miro					Miro Log4j Updates			
Mitel					Mitel Statement			

Vendor Product Version(s) Status Update Available	Vendor Link	Notes Other References	Last Updated
Vendor Product Version(s) Status Update Available  MobileIron Core All Versions Affected Yes	Vendor Link  https://forums.ivanti. com/s/article/Security-Bulletin-CVE-2021- 44228-Remote-code- injection-in- Log4j?language=en_US	The mitigation instructions listed in a subse-	12/20/21  12/20/21

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

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Mulesoft	Cloudhub		Affected	Yes	Apache Log4j2 vulnerability - December 2021	This advisory is available to account holders only and has not been reviewed		12/15/2021
Mulesoft	Anypoint Studio	7.x	Affected	Yes	Apache Log4j2 vulnerability - December 2021	by CISA. This advisory is available to account holders only and has not been reviewed by CISA.		12/15/2021
N-able Nagios NAKIVO					N-able Statement Nagios Statement NAKIVO Statement	v		
Neo4j	Neo4j Graph Database	Version $>4.2, <42.12$	Affected	No	TTTTT TO Statement			12/13/2021
Netcup NetGate PFSense Netwrix	Multiple NetApp products		Affected		https://security.netapp. com/advisory/ntap- 20211210-0007/ Netcup Statement NetGate PFSense Forum Netwrix Statement			
New Relic	Containerized Private Minion (CPM)	3.0.57	Fixed	Yes	NR21-04	New Relic is in the process of revising guidance/docum however the fix version remains sufficient.	Security Bulletin NR21-04 entation,	12-18-2021
New Relic	New Relic Java Agent	<7.4.3	Affected	Yes	https://docs.newrelic. com/docs/release- notes/agent-release- notes/java-release- notes/java-agent-743/	Initially fixed in 7.4.2, but additional vulnerability found	New Relic tracking, covers CVE-2021-44228, CVE-2021-45046	12/20/2021
NextCloud Nextflow  Nexus Group NI (National Instruments) Nice Software (AWS) EnginFRAME	Nextflow	21.04.0.5552	Not Affected		NextCloud Help https: //www.nextflow.io/ docs/latest/index.html Nexus Group Docs NI Support Link Nice Software EnginFRAME Link			12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
NinjaRMM					NinjaRMM Article	This advisory is available to customers only and has not been reviewed by CISA		
Nomachine NoviFlow					Nomachine Forums Noviflow Link	<i>5,</i> 01611		
Nulab	Backlog	N/A (SaaS)	Fixed		Nulab Blog Post			
Nulab	Backlog Enterprise (On-premises)	< 1.11.7	Fixed	Yes	Nulab Blog Post			
Nulab	Cacoo	N/A (SaaS)	Fixed		Nulab Blog Post			
Nulab	Cacoo Enterprise (On-premises)	< 4.0.4	Fixed	Yes	Nulab Blog Post			
Nulab Nutanix	Typetalk AHV	N/A (SaaS) All	Fixed Not Affected		Nulab Blog Post Nutanix Security			12/20/2021
					Advisory			, ,
Nutanix	AOS	LTS (including Prism Element), Community Edition	Not Affected		Nutanix Security Advisory			12/20/2021
Nutanix	AOS	STS (including Prism Element)	Fixed	Yes	Nutanix Security Advisory	Patched in 6.0.2.4, available on the Portal for		
download		12/20/2021	T			~		10/00/0001
Nutanix	Beam		Fixed		Nutanix Security Advisory	Saas- Based Procuct. See Advisory.		12/20/2021
Nutanix	BeamGov		Fixed		Nutanix Security Advisory	Saas- Based Procuct. See Advisory.		12/20/2021
Nutanix	Calm	All	Not Affected		Nutanix Security Advisory	V		12/20/2021
Nutanix	Calm Tunnel VM	All	Not Affected		Nutanix Security Advisory			12/20/2021
Nutanix	Collector	All	Not Affected		Nutanix Security Advisory			12/20/2021
Nutanix	Collector Portal		Fixed		Nutanix Security Advisory	Saas- Based Procuct. See Advisory.		12/20/2021
Nutanix	Data Lens		Not Affected		Nutanix Security Advisory	Saas- Based Procuct. See Advisory.		12/20/2021
Nutanix	Era	All	Not Affected		Nutanix Security			12/20/2021

Advisory

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Onespan Opengear OpenMRS TALK					Onespan Link Opengear Link OpenMRS TALK Link			
OpenNMS OpenSearch					OpenNMS Link OpenSearch Discussion Link			
OpenText					OpenText Log4J Remote Code Execution			12/23/2021
Oracle			Affected		Oracle Security Alert My Oracle Support Document	The support document is available to		12/17/2021
						customers only and has not been reviewed by CISA		
Orgavision Osirium	PAM		Not Affected		Orgavision Link Osirium statement			
Osirium Osirium OTRS OVHCloud OwnCloud	PEM PPA		Not Affected Not Affected		Osirium statement Osirium statement OTRS Link OVHCloud Blog Post OwnCloud Link			
OxygenXML	Author		Affected	Fixed	Yes	https://www.oxygenxml.		12/17/2021
						com/ security/ advisory/ CVE- 2021- 44228.		
OxygenXML	Developer		Affected	Fixed	Yes	html https: //www. oxygenxml.		12/17/2021
						com/ security/ advisory/ CVE- 2021- 44228.		
OxygenXML	Editor		Affected	Fixed	Yes	html https:		12/17/2021
						//www. oxygenxml. com/ security/ advisory/ CVE- 2021- 44228.		
OxygenXML	Oxygen Content Fusion	2.0, 3.0, 4.1	Affected	Fixed	Yes	html https: //www. oxygenxml. com/ security/ advisory/ CVE- 2021- 44228. html		12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
OxygenXML	Oxygen Feedback	1.4.4 & older	Affected	Fixed	Yes	https: //www.	12/17/2021
	Enterprise					$rac{ m oxygenxml.}{ m com}/$	
						security/	
						advisory/	
						CVE-	
						2021-	
						44228. html	
OxygenXML	Oxygen License	v22.1 to v24.0	Affected	Fixed	Yes	https:	12/17/2021
ONJ SCHITTINE	Server	V22.1 00 V21.0	Timecoca	1 mod	105	//www.	12/11/2021
						oxygenxml.	
						com/	
						security/	
						advisory/	
						CVE- 2021-	
						44228.	
						html	
${\bf OxygenXML}$	Oxygen PDF	$v22.1,\ 23.0,\ 23.1,\ 24.0$	Affected	Fixed	Yes	https:	12/17/2021
	Chemistry					//www.	
						oxygenxml.	
						com/	
						security/ advisory/	
						CVE-	
						2021-	
						44228.	
						$\operatorname{html}$	
OxygenXML	Oxygen SDK		Affected	Fixed	Yes	https:	12/17/2021
						//www.	
						$rac{ m oxygenxml.}{ m com}/$	
						security/	
						advisory/	
						CVE-	
						2021-	
						44228.	
OxygenXML	Plugins (see		Affected	Fixed	Yes	html https:	12/17/2021
OxygenAML	advisory link)		Affected	Fixed	165	//www.	12/11/2021
	davisory min)					oxygenxml.	
						com/	
						security/	
						advisory/	
						CVE-	
						2021- 44228.	
						html	
OxygenXML	Publishing		Affected	Fixed	Yes	https:	12/17/2021
	Engine					//www.	, ,
						oxygenxml.	
						com/	
						security/	
						advisory/ CVE-	
						2021-	
						44228.	
						html	

Affected   Fixed   Fixed   Fixed   Palantir   Palanti	All	Affected   Fixed   Fixed   Fixed   Palantir Response to Log4 Valuerability   Polluntir.com)   Palantir Response to Log4 Valuerability   Polluntir.com   Polluntir.com   Palantir Response to Log4 Valuerability   Polluntir.com   Palantir Response to Log4 Valuerability   Palantir Response to Log4 Valuerability   Palantir.com   Palantir Response to Log4 Valuerability   Palantir.com   Palantir Response to Log4 Valuerability   Palantir.com	Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
html	OxygenXML Weblief  Affected Fixed Yes https: 12/17/2021  //www.oxygenxml. com/ security/ advisory/ CVE- 2021- 44228. html Palantir Poundry  Palantir Foundry  Poundry  Palantir Foundry  Poundry  Poundry	Min   Min	OxygenXML	Web Author		Affected	Fixed	Yes	//www. oxygenxml. com/ security/ advisory/ CVE- 2021-	12/17/2021
Palantir Palantir All Fixed Palantir Response to No impact 12/19/2021  Foundry Log4j Vulnerability to (palantir.com) Palantir-hosted or Apolloconnected instances, and	Adaptic   All   Fixed   Palantir   Response to   No impact   12/19/2021	Palantir	OxygenXML	WebHelp		Affected	Fixed	Yes	html https: //www. oxygenxml. com/ security/ advisory/ CVE-	12/17/2021
	have been deployed for full re- mediation. Discon- nected customer instances may require	have been deployed for full remediation. Discon- nected customer instances may require manual updates.  Palantir All Fixed Palantir Response to Gotham  Fixed Palantir Response to Log4J Vulnerability (palantir.com) Palantir- hosted or Apollo- connected instances, and updates have been deployed			All	Fixed		Log4j Vulnerability	44228. html No impact to Palantir- hosted or Apollo- connected instances, and	12/19/2021

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Update
Palo-Alto	GlobalProtect		Not Affected		CVE-2021-44228			
Networks	App				Informational: Impact			
					of Log4j Vulnerability			
					CVE-2021-44228			
					(paloaltonetworks.com)			
Palo-Alto	Palo-Alto		Not Affected		CVE-2021-44228			
Networks	Networks-OS for		Tiou Illicoud		Informational: Impact			
TTOWOTES	Firewall and				of Log4j Vulnerability			
	Wildfire				CVE-2021-44228			
	Wildine				(paloaltonetworks.com)			
D-1- A14-	D.: A		NI - 4 A G 4 - 1					
Palo-Alto	Prisma Access		Not Affected		CVE-2021-44228			
Networks					Informational: Impact			
					of Log4j Vulnerability			
					CVE-2021-44228			
					(paloaltonetworks.com)			
Palo-Alto	Prisma Cloud		Not Affected		CVE-2021-44228			
Networks					Informational: Impact			
					of Log4j Vulnerability			
					CVE-2021-44228			
					(paloaltonetworks.com)			
Palo-Alto	Prisma Cloud		Not Affected		CVE-2021-44228			
Networks	Compute				Informational: Impact			
11001101110	Compare				of Log4j Vulnerability			
					CVE-2021-44228			
					(paloaltonetworks.com)			
Palo-Alto	Okyo Grade		Not Affected		CVE-2021-44228			
Networks	Okyo Grade		Not Affected		Informational: Impact			
Networks								
					of Log4j Vulnerability			
					CVE-2021-44228			
D 1 41	a a a .		37 . 100 . 1		(paloaltonetworks.com)			
Palo-Alto	SaaS Security		Not Affected		CVE-2021-44228			
Networks					Informational: Impact			
					of Log4j Vulnerability			
					CVE-2021-44228			
					(paloaltonetworks.com)			
Palo-Alto	WildFire		Not Affected		CVE-2021-44228			
Networks	Appliance				Informational: Impact			
	-				of Log4j Vulnerability			
					CVE-2021-44228			
					(paloaltonetworks.com)			
Palo-Alto	WildFire Cloud		Not Affected		CVE-2021-44228			
Networks			0 22200000		Informational: Impact			
					of Log4j Vulnerability			
					CVE-2021-44228			
					(paloaltonetworks.com)			
Palo-Alto	Han ID A mant		Not Affected					
	User-ID Agent		NOT Affected		CVE-2021-44228			
Networks					Informational: Impact			
					of Log4j Vulnerability			
					CVE-2021-44228			
					(paloaltonetworks.com)			
Panopto					Panopto Support Link			

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Power Admin LLC	PA File Sight	NONE	Not Affected		Update December 2021: None of our products (PA Server Monitor, PA Storage Monitor, PA File Sight and PA WatchDISK), and none of our websites, use log4j. One less thing to			12/17/2021
Power Admin LLC	PA Storage Monitor	NONE	Not Affected		worry about Update December 2021: None of our products (PA Server Monitor, PA Storage Monitor, PA File Sight and PA WatchDISK), and none of our websites, use log4j. One less thing to			12/17/2021
Power Admin LLC	PA Server Monitor	NONE	Not Affected		worry about Update December 2021: None of our products (PA Server Monitor, PA Storage Monitor, PA File Sight and PA WatchDISK), and none of our websites, use log4j. One less thing to			12/17/2021
Pretix PrimeKey Progress / IpSwitch ProofPoint					worry about Pretix Blog Post PrimeKey Support Link Progress / IpSwitch Link ProofPoint Article	This advisory is available for customers only and has not been reviewed by CISA		
ProSeS Prosys Proxmox PRTG Paessler					ProSeS Link Prosys News Link Proxmox Forum PRTG Paessler Link	5, 01011		
PTC	Axeda Platform	6.9.2	Affected	No	PTC Axeda Platform Apache log4j vulnerability - Incident Response			12/17/2021
PTC	ThingsWorx Platform	8.5,9.0,9.1,9.2, All supported versions	Affected	No	ThingWorx Apache log4j vulnerability - Incident Response			12/17/2021
PTC	ThingsWorx Analytics	8.5,9.0,9.1,9.2, All supported versions	Affected	No	ThingWorx Apache log4j vulnerability - Incident Response			12/17/2021
PTV Group Pulse Secure	Ivanti Connect Secure (ICS)		Not Affected		PTV Group Link Pulse Secure Article: KB44933 - CVE-2021-44228 - Java			
Pulse Secure	Ivanti Neurons for secure Access		Not Affected		logging library (log4j) Pulse Secure Article: KB44933 - CVE-2021-44228 - Java logging library (log4j)			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Pulse Secure	Ivanti Neurons for ZTA		Not Affected		Pulse Secure Article: KB44933 - CVE-2021-44228 - Java			
Pulse Secure	Pulse Connect Secure		Not Affected		logging library (log4j) Pulse Secure Article: KB44933 - CVE-2021-44228 - Java			
Pulse Secure	Pulse Desktop Client		Not Affected		logging library (log4j) Pulse Secure Article: KB44933 - CVE-2021-44228 - Java			
Pulse Secure	Pulse Mobile Client		Not Affected		logging library (log4j) Pulse Secure Article: KB44933 - CVE-2021-44228 - Java			
Pulse Secure	Pulse One		Not Affected		logging library (log4j) Pulse Secure Article: KB44933 - CVE-2021-44228 - Java			
Pulse Secure	Pulse Policy Secure		Not Affected		logging library (log4j) Pulse Secure Article: KB44933 - CVE-2021-44228 - Java			
Pulse Secure	Pulse Secure Services Director		Not Affected		logging library (log4j) Pulse Secure Article: KB44933 - CVE-2021-44228 - Java			
Pulse Secure	Pulse Secure Virtual Traffic Manager		Not Affected		logging library (log4j) Pulse Secure Article: KB44933 - CVE-2021-44228 - Java logging library (log4j)			
Pulse Secure	Pulse Secure Web Application Firewall		Not Affected		Pulse Secure Article: KB44933 - CVE-2021-44228 - Java logging library (log4j)			
Pulse Secure	Pulse ZTA		Not Affected		Pulse Secure Article: KB44933 - CVE-2021-44228 - Java logging library (log4j)			
Puppet Pure Storage					Puppet Blog Post Pure Storage Support Link	This advisory is available for customers only and has not been reviewed	5	
Pulse Secure	Ivanti Neurons for ZTA		Not Affected		Pulse Secure Article: KB44933 - CVE-2021-44228 - Java	by CISA		
Pulse Secure	Ivanti Neurons for secure Access		Not Affected		logging library (log4j) Pulse Secure Article: KB44933 - CVE-2021-44228 - Java logging library (log4j)			
Pure Storage	FlashBlade	3.1.x,3.2.x,3.3.x	Affected	No	Pure Storage Customer Portal	Patch expected 12/24/2022	1	12/15/2021
Pure Storage	Flash Array	5.3.x, 6.0.x, 6.1.x, 6.2.x	Affected	No	Pure Storage Customer Portal	Patch expected 12/20/2021		12/15/2021
Pure Storage	Cloud Blockstore	CBS6.1.x, CBS6.2.x	Affected	No	Pure Storage Customer Portal	Patch expected 12/27/2022		12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Pure Storage	Pure1	N/A	Fixed	Yes	Pure Storage Customer Portal			12/15/2021
Pure Storage Pyramid	PortWorx	2.8.0+	Affected	Yes	Pure Storage Customer Portal Pyramid Analytics			12/15/2021
Analytics QF-Test Qlik					Community Link QF-Test Blog Post Qlik Community Link			
QMATIC	Orchestra Central	6.0+	Not Affected		QMATIC Link			12/21/2021
QMATIC	Appointment Booking	2.4+	Affected	Yes	QMATIC Link	Update to v. 2.8.2 which contains log4j 2.16		12/21/2021
QMATIC	Insights	Cloud	Affected	Yes	QMATIC Link	log4j 2.16 log4j 2.16 applied 2021-12-16		12/21/2021
QMATIC	Appointment Booking	Cloud/Managed Service	Affected	Yes	QMATIC Link	log4j 2.16 applied 2021-12-15		12/21/2021
QNAP QOPPA QSC Q-SYS			Under Investigation		QNAP Security Advisory QOPPA Link QSC Q-SYS Article			
QT Quest Global R R2ediviewer	R	4.1.1	Not Affected Not Affected		QT Quest Global https://www.r- project.org/ R2ediviewer Link			12/21/2021
Radware Rapid7	AlcidekArt, kAdvisor, and kAudit	on-prem	Not Affected		Radware Support Link Rapid7 Statement			12/15/2021
Rapid7	AppSpider Enterprise	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	AppSpider Pro	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	Insight Agent	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	InsightAppSec Scan Engine	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	InsightAppSec Scan Engine	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7 Rapid7	InsightCloudSec/I InsightConnect	Dion-Mctond on-prem	Not Affected Not Affected		Rapid7 Statement Rapid7 Statement			$     \begin{array}{r}       12/15/2021 \\       12/15/2021    \end{array} $
Rapid7	Orchestrator InsightIDR	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	Network Sensor InsightIDR/Insigh	-	Not Affected		Rapid7 Statement			12/15/2021
паріцт	Collector & Event Sources	коффиси	Not Affected		Rapidi Statement			12/13/2021
Rapid7	InsightOps DataHub	InsightOps DataHub <= 2.0	Affected	Yes	Rapid7 Statement	Upgrade DataHub to version 2.0.1 using the following instruc- tions.		12/15/2021
Rapid7	InsightOps non-Java logging libraries	on-prem	Not Affected		Rapid7 Statement	V		12/15/2021
Rapid7	InsightOps r7insight_java	<=3.0.8	Affected	Yes	Rapid7 Statement	Upgrade r7insight_jav to 3.0.9	ra	12/15/2021
Rapid7	logging library InsightVM Kubernetes	on-prem	Not Affected		Rapid7 Statement	ю <b>э</b> .0.9		12/15/2021
Rapid7	Monitor InsightVM/Nexpo	sen-prem	Not Affected		Rapid7 Statement			12/15/2021

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Rapid7	Metasploit Pro	on-prem	Not Affected		Rapid7 Statement	Metasploit Pro ships with log4j but has specific configura- tions applied to it that mitigate Log4Shell. A future update will contain a fully patched version of log4j.		12/15/2021
Rapid7	tCell Java Agent	on-prem	Not Affected		Rapid7 Statement	10g4J.		12/15/2021
Rapid7 Raritan Ravelin Real-Time	Velociraptor  Distributed	on-prem	Not Affected  Not Affected		Rapid7 Statement Raritan Support Link Ravelin Link RTI Statement			12/15/2021 12/16/2021
Innovations (RTI) Real-Time Innovations	Logger Recording Console		Not Affected		RTI Statement			12/16/2021
(RTI) Real-Time Innovations (RTI)	RTI Administration Console		Not Affected		RTI Statement			12/16/2021
Real-Time Innovations (RTI)	RTI Code Generator		Not Affected		RTI Statement			12/16/2021
Real-Time Innovations (RTI)	RTI Code Generator Server		Not Affected		RTI Statement			12/16/2021
Real-Time Innovations (RTI)	RTI Micro Application Generator (MAG)	as part of RTI Connext Micro 3.0.0, 3.0.1, 3.0.2, 3.0.3	Affected		RTI Statement			12/16/2021
Real-Time Innovations (RTI)	RTI Micro Application Generator (MAG)	as part of RTI Connext Professional 6.0.0 and 6.0.1	Affected		RTI Statement			12/16/2021
Real-Time Innovations (RTI)	RTI Monitor		Not Affected		RTI Statement			12/16/2021
Red Hat	Red Hat JBoss Enterprise Application Platform	7	Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	Maven Patch - Affects only the Mavenized distribu- tion. Container, Zip and RPM distro aren't affected.		Dec/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Red Hat	Red Hat Process Automation	7	Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	Maven Patch - Affects	$\mathrm{Dec}/21/2021$
						only the Mavenized	
						distribu- tion.	
						Container, Zip and	
						RPM distro	
						aren't affected.	
ded Hat	Red Hat CodeReady Studio	12.21.0	Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	CRS 12.21.1 Patch	$\mathrm{Dec}/21/2021$
ed Hat	Red Hat Data Grid	8	Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	RHSA- 2021:5132	$\mathrm{Dec}/21/2021$
Red Hat	Red Hat Integration		Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	RHSA- 2021:5130	$\mathrm{Dec}/21/2021$
Red Hat	Camel K Red Hat Integration		Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	RHSA- 2021:5126	$\mathrm{Dec}/21/2021$
Red Hat	Camel Quarkus Red Hat JBoss		Fixed	Yes	CVE-2021-44228- Red	RHSA-	$\mathrm{Dec}/21/2021$
ted Hat	A-MQ Streaming		Fixed	165	Hat Customer Portal	2021:5138	Dec/21/2021
Red Hat	Red Hat JBoss Fuse	7	Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	RHSA- 2021:5134	$\mathrm{Dec}/21/2021$
Red Hat	Red Hat Vert.X	4	Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	RHSA- 2021:5093	$\mathrm{Dec}/21/2021$
Red Hat OpenShift Container Platform 3.11	openshift3/ose- logging- elasticsearch5		Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	RHSA- 2021:5094	$\mathrm{Dec}/21/2021$
ed Hat penShift	openshift4/ose- logging-		Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	Please refer to	$\mathrm{Dec}/21/2021$
${ m Container} \ { m Clatform} \ 4$	elasticsearch6					Red Hat Customer	
						Portal to find the	
						right errata for	
						your version.	
Red Hat OpenShift	openshift4/ose- metering-hive		Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	Please refer to	$\mathrm{Dec}/21/2021$
Container Clatform 4						Red Hat Customer	
						Portal to find the	
						right errata for	
0 - 1 II +	1.6.4/		T): 1	V	CN/E 2021 44222 P. 1	your version.	D /01/0001
Red Hat OpenShift	openshift4/ose- metering-presto		Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	Please refer to	$\mathrm{Dec}/21/2021$
Container Platform 4						Red Hat Customer	
						Portal to find the	
						right errata for	
						your version.	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Red Hat OpenShift Logging	logging- elasticsearch6- container		Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	Please refer to Red Hat Customer Portal to find the right errata for your	Dec/21/2021
Red Hat	Red Hat Single	7	Not Affected		CVE-2021-44228- Red Hat Customer Portal	version.	$\mathrm{Dec}/21/2021$
Red Hat	Sign-On Red Hat Enterprise Linux	6	Not Affected		CVE-2021-44228- Red Hat Customer Portal		$\mathrm{Dec}/20/2021$
Red Hat	Red Hat Enterprise Linux	7	Not Affected		CVE-2021-44228- Red Hat Customer Portal		$\mathrm{Dec}/20/2021$
Red Hat	Red Hat Enterprise Linux	8	Not Affected		CVE-2021-44228- Red Hat Customer Portal		$\mathrm{Dec}/20/2021$
Red Hat	Red Hat build of Quarkus		Not Affected		CVE-2021-44228- Red Hat Customer Portal		$\mathrm{Dec}/20/2021$
Red Hat	Red Hat Decision Manager	7	Not Affected		CVE-2021-44228- Red Hat Customer Portal		$\mathrm{Dec}/20/2021$
Red Hat Software Collections	rh-java- common-log4j		Not Affected		CVE-2021-44228- Red Hat Customer Portal		$\mathrm{Dec}/21/2021$
Red Hat Software Collections	rh-maven $35$ - $log4j12$		Not Affected		CVE-2021-44228- Red Hat Customer Portal		$\mathrm{Dec}/21/2021$
Red Hat Software Collections	rh-maven $36$ - $\log 4$ j $12$		Not Affected		CVE-2021-44228- Red Hat Customer Portal		$\mathrm{Dec}/21/2021$
Red Hat	$\log 4$ j-core		Not Affected		CVE-2021-44228- Red Hat Customer Portal		$\mathrm{Dec}/21/2021$
Red Hat	Satellite 5		Not Affected		CVE-2021-44228- Red Hat Customer Portal		$\mathrm{Dec}/21/2021$
Red Hat	Spacewalk		Not Affected		CVE-2021-44228- Red Hat Customer Portal		$\mathrm{Dec}/21/2021$
Red Hat	Red Hat JBoss Enterprise Application Platform Expansion Pack	7	Not Affected		CVE-2021-44228- Red Hat Customer Portal		Dec/20/2021
Red Hat OpenStack Platform 13 (Queens) Red5Pro	opendaylight		Affected	No	CVE-2021-44228- Red Hat Customer Portal	End of Life	$\mathrm{Dec}/21/2021$
RedGate ResMed ResMed Redis Reiner SCT ReportURI Respondus	myAir AirView		Not Affected Not Affected		RedGate Link ResMed Advisory Link ResMed Advisory Link Redis Link Reiner SCT Forum ReportURI Link Respondus Support Link	This advisory is available to customers only and has not been reviewed by CISA	12/21/2021 12/21/2021

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

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

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Salesforce	Evergage		Affected		Salesforce Statement	"Evergage		12/15/2021
	(Interaction					(Interac-		• •
	Studio)					tion		
	,					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		
G 1 6			1.00			steps."		10/17/0001
Salesforce	Force.com	ce.com	Affected		Salesforce Statement	"Force.com		12/15/2021
						is reported		
						to be		
						affected by		
					CVE-2021-			
						44228.		
						The		
						service is		
						being		
						updated to		
						remediate		
						the vulner-		
						ability		
						identified		
						$_{ m in}$		
						CVE-2021-		
						44228."		
Salesforce	Heroku		Not Affected		Salesforce Statement	"Heroku is		12/15/2021
2010210100	11010101		1.00 11110000			reported		//
						to not be		
						affected by		
						CVE-2021-		
						44228; no		
						further		
						action is		
						necessary at this		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Salesforce	Marketing Cloud	Version(s)	Affected	Update Available	Salesforce Statement	"Marketing Cloud is reported to be affected by CVE-2021-44228. The service is being updated to remediate the vulnerability identified in		12/15/2021
Salesforce	MuleSoft (Cloud)		Affected		Salesforce Statement	CVE-2021- 44228." "MuleSoft (Cloud) is		12/15/2021
Salesforce	MulaCaft		II. lan arma		Salasfana Statament	reported to be affected by CVE-2021-44228. The service is being updated to remediate the vulnerability identified in CVE-2021-44228."		19/15/2021
	MuleSoft (On-Premise)		Unknown		Salesforce Statement	"Please contact Customer Support."		12/15/2021
Salesforce	Pardot		Affected		Salesforce Statement	"Pardot is reported to be affected by CVE-2021-44228. The service is being updated to remediate the vulnerability identified in CVE-2021-44228."		12/15/2021

Cloud is reported to be affected by CVE-2021- 44228.	Cloud is reported to be affected by CVE-2021-
Salesforce Service Cloud Affected Salesforce Statement "Service Cloud is reported to be affected by CVE-2021- 44228."  Salesforce Statement "Service (Statement Cloud is reported to be affected by CVE-2021- 44228.  The service is	Salesforce       Service Cloud       Affected       Salesforce Statement       CVE-2021- 44228."       Service Cloud is reported to be service is being updated to remediate the vulner-ability distinction of the vulner-ability d
1	updated to remediate the vulnerability identified in CVE-2021-44228."  esforce Slack Affected Salesforce Statement "Slack is reported to be $0$

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

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Affected				pdf, CSAF	Siemens	12/19/2021
	Products					requests:	
						See pdf for	
						the	
						complete	
						list of	
						affected	
						products,	
						CSAF for	
						automated	
						parsing of data	
Siemens	Affected				pdf, CSAF	Siemens	12/21/2021
Energy	Products				pdi, CSAF	requests:	12/21/2021
Energy	Troducts					See pdf for	
						the	
						complete	
						list of	
						affected	
						products,	
						CSAF for	
						automated	
						parsing of	
						data	
Siemens	Affected				pdf, CSAF	Siemens	12/20/2021
Energy	Products					requests:	
						See pdf for	
						the	
						complete	
						list of	
						affected	
						products,	
						CSAF for	
						automated	
						parsing of data	
Siemens	Affected				pdf, CSAF	Siemens	12/16/2021
Energy	Products				pui, CSAI	requests:	12/10/2021
Lifergy	Troducts					See pdf for	
						the	
						complete	
						list of	
						affected	
						products,	
						CSAF for	
						automated	
						parsing of	
						data	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens Healthineers	ATELLICA DATA MANAGER v1.1.1 / v1.2.1 / v1.3.1		Affected	See Notes	Siemens Healthineers	If you have determined that your Atellica Data Manager has a "Java communication engine" service, and you require an immediate mitigation, then please contact your Siemens Customer Care Center or your local Siemens technical support	12/22/2021
Siemens Healthineers	CENTRALINK v16.0.2 / v16.0.3		Affected	See Notes	Siemens Healthineers	representative.  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 techni-	12/22/2021
Siemens Healthineers	DICOM Proxy VB10A		Affected	See Notes	Siemens Healthineers	cal support representative. Workaround: remove the vulnerable class from	12/22/2021
Siemens	Somatom Scope		Affected	See Notes	Siemens Healthineers	the .jar file evaluation	12/22/2021
Healthineers	Som 5 VC 50					ongoing	
Siemens Healthineers	Somatom Emotion Som5 VC50		Affected	See Notes	Siemens Healthineers	evaluation ongoing	12/22/2021

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

Vendor	Product Vers	rsion(s) Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	go.Sim, Som10	Affected	See Notes	Siemens Healthineers	Workaround:	12/22/2021
Healthineers	VA30 / VA40				In the	
					meantime,	
					we recom-	
					mend	
					preventing	
					access to	
					port 8090	
					from other	
					devices by	
					configura-	
					tion of the	
					hospital	
					network.	
Siemens	go.Top, Som10	Affected	See Notes	Siemens Healthineers	Workaround:	12/22/2021
		Affected	See Notes	Siemens Heartinneers		12/22/2021
Healthineers	VA20 /				In the	
	$VA20A\_SP5$ /				meantime,	
	VA30 / VA40				we recom-	
					mend	
					preventing	
					access to	
					port 8090	
					from other	
					devices by	
					configura-	
					tion of the	
					hospital	
					network.	
Siemens	go.Up, Som10	Affected	See Notes	Siemens Healthineers	Workaround:	12/22/2021
Healthineers	VA10 / VA20 /				In the	, ,
	VA10 / VA20 / VA30 / VA40				meantime,	
					we recom-	
					mend	
					preventing	
					access to	
					port 8090	
					from other	
					devices by	
					configura-	
					tion of the	
					hospital	
a.	164 CATE CATE		0.37	A	network.	
Siemens	MAGNETOM	Affected	See Notes	Siemens Healthineers	LOG4J is	12/22/2021
Healthineers	AERA $1,5T$ ,				used in the	
	MAGNETOM				context of	
	PRISMA,				the help	
	MAGNETOM				system.	
					Workaround:	
	PRISMA FIT,				close port	
					close born	
	MAGNETOM				8090 for	
	MAGNETOM SKYRA 3T				4 1 1	
	MAGNETOM SKYRA 3T NUMARIS/X				standalone	
	MAGNETOM SKYRA 3T				systems.	
	MAGNETOM SKYRA 3T NUMARIS/X				systems. Setup IP	
	MAGNETOM SKYRA 3T NUMARIS/X				systems.	
	MAGNETOM SKYRA 3T NUMARIS/X				systems. Setup IP whitelist-	
	MAGNETOM SKYRA 3T NUMARIS/X				systems. Setup IP whitelist- ing for	
	MAGNETOM SKYRA 3T NUMARIS/X				systems. Setup IP whitelist- ing for "need to	
	MAGNETOM SKYRA 3T NUMARIS/X				systems. Setup IP whitelist- ing for "need to access"	
	MAGNETOM SKYRA 3T NUMARIS/X				systems. Setup IP whitelist- ing for "need to access" systems to	
	MAGNETOM SKYRA 3T NUMARIS/X				systems. Setup IP whitelist- ing for "need to access" systems to network	
	MAGNETOM SKYRA 3T NUMARIS/X				systems. Setup IP whitelist- ing for "need to access" systems to network port 8090	
	MAGNETOM SKYRA 3T NUMARIS/X				systems. Setup IP whitelist- ing for "need to access" systems to network	
	MAGNETOM SKYRA 3T NUMARIS/X				systems. Setup IP whitelist- ing for "need to access" systems to network port 8090 in case a	
	MAGNETOM SKYRA 3T NUMARIS/X				systems. Setup IP whitelist- ing for "need to access" systems to network port 8090	

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

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

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens Healthineers	syngo.via VB20A / VB20A_HF01 - HF08 / VB20A_HF91 / VB20B / VB30A / VB30A_HF01 - VB30A_HF01 - VB30A_HF91VB. / VB30B_HF01 / VB40A / VB40A_HF01 - HF02 /VB40B / VB40B_HF01 - HF05 / VB50A / VB50A_CUT / VB50A_D4VB501 / VB50B_HF01 - HF03 / VB60A / VB60A_CUT / VB60A_D4 /		Affected	See Notes	Siemens Healthineers	Workaround: remove the vulnerable class from the .jar file	12/22/2021
Siemens Healthineers	VB60A_HF01 SENSIS DMCC / DMCM / TS / VM / PPWS / DS VD12A		Affected	See Notes	Siemens Healthineers	evaluation ongoing	12/22/2021
Siemens Healthineers	Cios Select FD/I.I. VA21 / VA21-S3P		Affected	See Notes	Siemens Healthineers	evaluation ongoing	12/22/2021
Siemens Healthineers	Cios Flow S1 / Alpha / Spin VA30		Affected	See Notes	Siemens Healthineers	evaluation ongoing	12/22/2021
Siemens Healthineers	syngo.via WebViewer VA13B / VA20A / VA20B		Affected	See Notes	Siemens Healthineers	Workaround: remove the vulnerable class from the .jar file	12/22/2021
Siemens Healthineers	X.Ceed Somaris 10 VA40*		Affected	See Notes	Siemens Healthineers	Workaround: In the meantime, we recom- mend preventing access to port 8090 from other devices by configura- tion of the hospital network.	12/22/2021
Siemens Healthineers	X.Cite Somaris 10 VA30/VA40		Affected	See Notes	Siemens Healthineers	Workaround: In the meantime, we recom- mend preventing access to port 8090 from other devices by configura- tion of the hospital network.	12/22/2021

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

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

Vendor	Product Version(s)	Status Update Available	Vendor Link	Notes Other References	Last Updated
SonicWall	SMA 100	Not Affected	Security Advisory	Log4j2 not	12/12/2021
			(sonicwall.com)	used in the	
				SMA100 appliance.	
SonicWall	SMA 1000	Not Affected	Security Advisory	Version	12/12/2021
			(sonicwall.com)	12.1.0 and	
				12.4.1 doesn't	
				use a	
				vulnerable version	
SonicWall	SonicCore	Not Affected	Security Advisory	SonicCore	12/12/2021
			(sonicwall.com)	doesn't	, ,
				use a $\text{Log4j2}$	
SonicWall	SonicWall	Not Affected	Security Advisory	Log4j2 Log4j2 not	12/12/2021
	Switch		(sonicwall.com)	used in the	, ,
				SonicWall Switch.	
SonicWall	WAF	Under	Security Advisory	Under	12/12/2021
		Investigation	(sonicwall.com)	Review	
SonicWall	WNM	Not Affected	Security Advisory (sonicwall.com)	Log4j2 not used in the	12/12/2021
			(somewan.com)	WNM.	
${\bf Sonic Wall}$	WXA	Not Affected	Security Advisory	WXA	12/12/2021
			(sonicwall.com)	doesn't use a	
				vulnerable	
				version	
Sophos	Cloud Optix	Fixed	Advisory: Log4J zero-day vulnerability	Users may have	12/12/2021
			AKA Log4Shell	noticed a	
			(CVE-2021-44228)	brief	
			Sophos	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	
Sophos	Reflexion	Not Affected	Advisory: Log4J	impacted. Reflexion	12/12/2021
Борнов		100 11100000	zero-day vulnerability	does not	12/12/2021
			AKA Log4Shell	run an ex-	
			(CVE-2021-44228) Sophos	ploitable configuration.	
Sophos	SG UTM (all	Not Affected	Advisory: Log4J	Sophos SG	12/12/2021
	versions)		zero-day vulnerability	UTM does	
			AKA Log4Shell (CVE-2021-44228)	not use Log4j.	
			Sophos		
Sophos	SG UTM All versions Manager (SUM)	Not Affected	Advisory: Log4J	SUM does	12/12/2021
	Manager (SUM) (all versions)		zero-day vulnerability AKA Log4Shell	not use Log4j.	
	` '		(CVE-2021-44228)	~ *	
			Sophos		

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

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

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

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

STERIS Advisory Link STERIS Advisory Link	12/22/2021 12/22/2021
	12/22/2021
	12/22/2021
STERIS Advisory Link	
STERIS Advisory Link	
	12/22/2021
	7 7 -
STERIS Advisory Link	12/22/2021
STERIS Advisory Link	12/22/2021
STERIS Advisory Link	12/22/2021
STERIS Advisory Link	12/22/2021
	,,
STERIS Advisory Link	12/22/2021
STERUS Advisory Link	12/22/2021
STERIS Advisory Link	12/22/2021
	, ,
STERIS Advisory Link	12/22/2021
STERIS Advisory Link	12/22/2021
STERIS Advisory Link	12/22/2021
CENTRAL ALL ALL ALL ALL ALL ALL ALL ALL ALL	10/00/001
STERIS Advisory Link	12/22/2021
STERIS Advisory Link	12/22/2021
	STERIS Advisory Link  STERIS Advisory Link

Vendor	Product Version(s)	Status Update Available	Vendor Link Notes Other References	Last Updated
STERIS	AMSCO	Not Affected	STERIS Advisory Link	12/22/2021
	EVOLUTION MEDIUM			
	STEAM			
	STERILIZER			
STERIS	CELERITY HP INCUBATOR	Not Affected	STERIS Advisory Link	12/22/2021
STERIS	CELERITY	Not Affected	STERIS Advisory Link	12/22/2021
	STEAM			, ,
STERIS	INCUBATOR VERIFY	Not Affected	STERIS Advisory Link	12/22/2021
STEMS	INCUBATOR	Not Affected	STERIS Advisory Link	12/22/2021
	FOR ASSERT			
	SELF- CONTAINED			
	BIOLOGICAL			
	INDICATORS			
STERIS	SYSTEM 1	Not Affected	STERIS Advisory Link	12/22/2021
	endo LIQUID CHEMICAL			
	STERILANT			
	PROCESSING SYSTEM			
STERIS	V-PRO 1 LOW	Not Affected	STERIS Advisory Link	12/22/2021
	TEMPERA-		·	, ,
	TURE STERILIZA-			
	TION			
	SYSTEM			
STERIS	V-PRO 1 PLUS LOW TEM-	Not Affected	STERIS Advisory Link	12/22/2021
	PERATURE			
	STERILIZA-			
	TION SYSTEM			
STERIS	V-PRO MAX 2	Not Affected	STERIS Advisory Link	12/22/2021
	LOW TEM-			
	PERATURE STERILIZA-			
	TION			
CONTRACT	SYSTEM	N A.C 1	CONTROL A 1	19/99/9991
STERIS	V-PRO MAX LOW TEM-	Not Affected	STERIS Advisory Link	12/22/2021
	PERATURE			
	STERILIZA-			
	TION SYSTEM			
STERIS	V-PRO S2	Not Affected	STERIS Advisory Link	12/22/2021
	LOW TEM-			
	PERATURE STERILIZA-			
	TION			
CTEDIC	SYSTEM SecureCare	Not Affected	OTEDIC Advisors Link	19 /99 /9091
STERIS	ProConnect	Not Affected	STERIS Advisory Link	12/22/2021
	Technical			
	Support Services			
STERIS	HexaVue	Not Affected	STERIS Advisory Link	12/22/2021
	Integration		·	, ,
STERIS	System IDSS	Not Affected	STERIS Advisory Link	12/22/2021
STEUIS	Integration	Not Allected	STERUS Advisory Link	12/22/2021
	System			
STERIS	Harmony iQ Integration	Not Affected	STERIS Advisory Link	12/22/2021
	Systems			
STERIS	HexaVue	Not Affected	STERIS Advisory Link	12/22/2021

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other Reference	ees Last Updated
Tableau	Tableau Prep Builder	The following versions and lower: 22021.4.1, 2021.3.2, 2021.2.2, 2021.1.4, 2020.4.1, 2020.3.3, 2020.2.3, 2020.1.5, 2019.4.2, 2019.3.2, 2019.2.3, 2019.1.4, 2018.3.3	Affected	Yes	Apache Log4j2 vulnerability (Log4shell)		12/22/2021
Tableau	Tableau Public Desktop Client	The following versions and lower: 2021.4	Affected	Yes	Apache Log4j2 vulnerability (Log4shell)		12/22/2021
Γableau	Tableau Reader	The following versions and lower: 2021.4	Affected	Yes	Apache Log4j2 vulnerability (Log4shell)		12/22/2021
Tableau	Tableau Bridge	The following versions and lower: 20214.21.1109.1748, 20213.21.1112.1434, 20212.21.0818.1843, 20211.21.0617.1133, 20204.21.0217.1203, 20203.20.0913.2112, 20202.20.0721.1350, 20201.20.0614.2321, 20194.20.0614.2307, 20193.20.0614.2306, 20192.19.0917.1648, 20191.19.0402.1911, 20183.19.0115.1143	Affected	Yes	Apache Log4j2 vulnerability (Log4shell)		12/22/2021
Γalend		20100.10.0110.1140			https://jira.talendforge. org/browse/TCOMP- 2054		
Tanium TealiumIQ TeamPasswor	All dManager	All versions	Not Affected		Tanium Statement  TealiumIQ Security Update TeamPasswordManager Blog	Tanium does not use Log4j.	12/21/2021
Teamviewer Tech Software	OneAegis (f/k/a IRBManager)	All versions	Not Affected		TeamViewer Bulletin Log4j CVE-2021-44228 Vulnerability Impact Statement	OneAegis does not	12/15/2021
Гесh Software	SMART	All versions	Not Affected		Log4j CVE-2021-44228 Vulnerability Impact Statement	use Log4j. SMART does not	12/15/2021
Tech Software	Study Binders	All versions	Not Affected		Log4j CVE-2021-44228 Vulnerability Impact Statement	use Log4j. Study Binders does not use Log4j.	12/15/2021
TechSmith Telestream Tenable	Tenable.io / Nessus		Not Affected		TechSmith Article Telestream Bulletin Tenable log4j Statement	None of Tenable's products are running the version of Log4j vulnerable to CVE-2021- 44228 or CVE-2021- 45046 at this time	

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

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

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

Vendor Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Thomson HighQ Reuters Appliance	<3.5	Affected	Yes	https://highqsolutions.zendesk.com	Reported by vendor - Documentation is in vendor's client portal (login required). This advisory is available to customer only and has not been reviewed		12/20/2021
${\bf Threat Locker}$				ThreatLocker Log4j Statement	by CISA.		
ThycoticCentrifySecret Serv	ver N/A	Not Affected		ThycoticCentrify Products NOT Affected by CVE-2021-44228 Exploit			12/10/21
$\begin{tabular}{ll} Thy cotic Centrify Privilege\\ Manager \end{tabular}$	N/A	Not Affected		ThycoticCentrify Products NOT Affected by CVE-2021-44228 Exploit			12/10/21
$\begin{array}{c} {\bf ThycoticCentrifyAccount}\\ {\bf Lifecycle}\\ {\bf Manager} \end{array}$	N/A	Not Affected		ThycoticCentrify Products NOT Affected by CVE-2021-44228 Exploit			12/10/21
$\begin{array}{c} {\bf Thy cotic Centrify Privileged} \\ {\bf Behavior} \\ {\bf Analytics} \end{array}$	N/A	Not Affected		ThycoticCentrify Products NOT Affected by CVE-2021-44228 Exploit			12/10/21
ThycoticCentrifyDevOps Se Vault	crets N/A	Not Affected		ThycoticCentrify Products NOT Affected by CVE-2021-44228 Exploit			12/10/21
ThycoticCentrifyConnection Manager	n N/A	Not Affected		ThycoticCentrify Products NOT Affected by CVE-2021-44228 Exploit			12/10/21
ThycoticCentrifyPassword I Server	Reset N/A	Not Affected		ThycoticCentrify Products NOT Affected by CVE-2021-44228 Exploit			12/10/21
ThycoticCentrifyCloud Suit Tibco Top Gun Technology (TGT)	e N/A	Not Affected		ThycoticCentrify Products NOT Affected by CVE-2021-44228 Exploit Tibco Support Link TGT Bulletin			12/10/21
TopDesk	yHub All	Not Affected		TopDesk Statement Topicus Keyhub Statement Topix Statement Tosibox Security Advisory			2021-12-20

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
TPLink	Omega Controller	Linux/Windows(all)	Affected	Yes	Statement on Apache Log4j Vulnerability	Update is Beta. Reddit: 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	12/15/2021
Tricentis Tosca	All		Under Investigation		https://success. trendmicro.com/ solution/000289940 Tricentis Tosca Statement	2.10		
Tripwire Trimble	eCognition	10.2.0 Build 4618	Affected	No	Tripwire Log4j Statement Details are shared with active subscribers	Remediation steps provided by Trimble		12/23/2021
TrueNAS Tufin TYPO3 Ubiquiti	UniFi Network Application	6.5.53 & lower versions	Affected	Yes	TrueNAS Statement Tufin Statement TYPO3 Statement UniFi Network Application 6.5.54	by 17thhole		
Ubiquiti	UniFi Network Controller	6.5.54 & lower versions	Affected	Yes	Ubiquiti Community UniFi Network Application 6.5.55 Ubiquiti Community		6.5.54 is reported to still be vulnerable. 6.5.55 is the new recommendation for mitigatin log4j vulnerabilities by updating to log4j 2.16.0	12/15/2021
Ubuntu Umbraco					Ubuntu Security Advisory Umbraco Security Advisory			
Uniflow Unify ATOS Unimus USSIGNAL MSP					UniFlow Security Advisory Unify ATOS Advisory Unimus Statement USSIGNAL MSP Statement			
VArmour Varian	Acuity	All	Under Investigation		VArmour Statement Varian Advisory Link			12/22/2021
/arian	DITC	All	Under Investigation		Varian Advisory Link			12/22/2021
Varian	ARIA Connect (Cloverleaf)	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	ARIA oncology information system for Medical Oncology	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	XMediusFax for ARIA oncology information system for Medical Oncology	All	Under Investigation		Varian Advisory Link			12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	I	ast Updated
Varian	ARIA oncology information system for Radiation	All	Not Affected		Varian Advisory Link			1	2/22/2021
Varian	Oncology ARIA eDOC	All	Not Affected		Varian Advisory Link			1	2/22/2021
varian Varian	XMediusFax for	All	Under		Varian Advisory Link Varian Advisory Link				2/22/2021
varian	ARIA oncology information system for Radiation Oncology	All	Investigation		varian Advisory Ellik			1	2/22/2021
Varian	ARIA Radiation Therapy Management System (RTM)		Not Affected		Varian Advisory Link				2/22/2021
Varian	Bravos Console	All	Not Affected		Varian Advisory Link			1	2/22/2021
Varian	Clinac	All	Under Investigation		Varian Advisory Link				2/22/2021
Varian	Cloud Planner	All	Not Affected		Varian Advisory Link				2/22/2021
Varian	DoseLab	All	Not Affected		Varian Advisory Link				2/22/2021
Varian	Eclipse treatment planning software	All	Not Affected		Varian Advisory Link				2/22/2021
Varian	ePeerReview	All	Under Investigation		Varian Advisory Link				2/22/2021
Varian	Ethos	All	Not Affected		Varian Advisory Link				2/22/2021
Varian	FullScale oncology IT solutions	All	Under Investigation		Varian Advisory Link			1	2/22/2021
Varian	Halcyon system	All	Under Investigation		Varian Advisory Link			1	2/22/2021
Varian	Identify	All	Not Affected		Varian Advisory Link				2/22/2021
Varian	Information Exchange Manager (IEM)	All	Not Affected		Varian Advisory Link			1	2/22/2021
Varian	InSightive	All	Under		Varian Advisory Link			1	2/22/2021
Varian	Analytics Large Integrated Oncology Network (LION)	All	Investigation Not Affected		Varian Advisory Link			1	2/22/2021
Varian	ICAP	All	Not Affected		Varian Advisory Link			1	2/22/2021
Varian	Mobius3D platform	All	Not Affected		Varian Advisory Link Varian Advisory Link				2/22/2021
Varian	ProBeam	All	Not Affected		Varian Advisory Link			1	2/22/2021
Varian	Qumulate	All	Not Affected		Varian Advisory Link				2/22/2021
Varian	Real-time Position Management (RPM)	All	Not Affected		Varian Advisory Link				2/22/2021
Varian	Respiratory Gating for Scanners (RGSC)	All	Not Affected		Varian Advisory Link			1	2/22/2021
Varian	SmartConnect solution	All	Affected		Varian Advisory Link	See Knowledge Article: 000038850 on MyVarian		1	2/22/2021

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
VMware	VMware HCX	4.x, 3.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
/Mware	VMware Horizon	8.x, 7.x	Affected	Yes	VMSA-2021-0028.4 (vmware.com)		VMware KB 87073 (vmware.com)	12/17/2021
/Mware	VMware Horizon Cloud Connector	1.x, 2.x	Affected	Yes	VMSA-2021-0028.1 (vmware.com)			12/12/2021
/Mware	VMware Horizon DaaS	9.1.x, 9.0.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
/Mware	VMware Identity Manager	3.3.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
Mware	VMware NSX-T Data Centern	3.x, 2.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
Mware	VMware Site Recovery Manager	8.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
Mware		2.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
Mware	VMware Tanzu GemFire	9.x, 8.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
/Mware	VMware Tanzu Greenplum	6.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
VMware	-	1.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
Mware		3.x, 2.x	Affected	Yes	VMSA-2021-0028.1 (vmware.com)			12/12/2021
Mware		2.x	Affected	Yes	VMSA-2021-0028.1 (vmware.com)			12/12/2021
Mware		2.x, 1.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
Mware	VMware Telco Cloud Automation	2.x, 1.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
Mware	VMware Unified Access Gateway	21.x, 20.x, 3.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
Mware	VMware vCenter Cloud Gateway	1.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
Mware	vCenter Server - OVA	7.x, 6.7.x, 6.5.x	Affected	Pending	VMSA-2021-0028.4 (vmware.com)	Workaround @ KB87081 (vmware.com	<b>5)</b>	2021-12-17
<sup>7</sup> Mware	vCenter Server - Windows	6.7.x, 6.5.x	Affected	Pending	VMSA-2021-0028.4 (vmware.com)	Workaround  @  KB87096  (vmware.com		2021-12-17
Mware	VMware vRealize Automation	8.x, 7.x	Affected	No	VMSA-2021-0028.1 (vmware.com)	(vinware.com	1)	12/12/2021
Mware	VMware vRealize Lifecycle Manager	8.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
Mware	VMware vRealize Log Insight	8.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021
Mware	VMware vRealize Operations	8.x	Affected	No	VMSA-2021-0028.1 (vmware.com)			12/12/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
VMware	VMware vRealize Operations Cloud Proxy	Any	Affected	No	VMSA-2021-0028.1 (vmware.com)		12/12/2021
VMware	VMware vRealize Orchestrator	8.x, 7.x	Affected	No	VMSA-2021-0028.1 (vmware.com)		12/12/2021
VMware	VMware Workspace ONE Access	21.x, 20.10.x	Affected	No	VMSA-2021-0028.1 (vmware.com)		12/12/2021
VMware	VMware Workspace ONE Access Connector (VMware Identity Manager Connector)	21.x, 20.10.x, 19.03.0.1	Affected	No	VMSA-2021-0028.1 (vmware.com)		12/12/2021
Vyaire WAGO	WAGO Smart	4.2.x < 4.8.1.3	Not Affected Affected	Yes	Vyaire Advisory Link WAGO Website		$     \begin{array}{r}       12/22/2021 \\       12/17/2021     \end{array} $
WAGO	Script	4.2.1 < 4.0.1.9	Affected	165	WAGO Website		12/11/2021
Wallarm Wasp Barcode technologies					Lab Mitigation Update Waspbarcode Assetcloud Inventorycloud		
WatchGuard Western Digital	Secplicity				Secplicity Critical RCE Westerndigital Product Security		
WIBU Systems	CodeMeter Keyring for TIA Portal	1.30 and prior	Affected	Yes	WIBU Systems Advisory Link	Only the Password Manager is affected	12/22/2021
WIBU Systems WindRiver WireShark Wistia WitFoo WordPress Worksphere Wowza	CodeMeter Cloud Lite	2.2 and prior	Affected	Yes	WIBU Systems Advisory Link Windriver Security Notice Gitlab Wireshark Wistia Incidents Witfoo Emergency Update Wordpress Support Workspace Security Update Wowza Known Issues with Streaming Engine		12/22/2021
WSO2	WSO2 Enterprise Integrator	6.1.0 and above	Affected	Yes	https://docs.wso2.com/ pages/viewpage.action? pageId=180948677	A temporary mitigation is available while vendor works on update	
XCP-ng					XCP lOG4j Vulnerability	-	
XenForo Xerox					Xenforo PSA Elasticsearch Xerox Special Bulletin		
XPertDoc XPLG XWIKI					CVE-2021-44228  Xpertdoc  XPLG Secure Log4j  Xwiki CVE-2021-44228		
Xylem Xylem Xylem	Aquatalk Avensor Sensus		Affected Affected	Pacthing complete Pacthing complete Pacthing complete	Xylem Advisory Link Xylem Advisory Link Xylem Advisory Link		$\begin{array}{c} 12/22/2021 \\ 12/22/2021 \\ 12/22/2021 \end{array}$
Ayıem	Sensus Analytics		Affected	ractning complete	Ayıem Advisory Link		12/22/2021

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Zenoss					Zenoss			
Zentera	CoIP Access	All	Not Affected		[CVE-2021-44228]			12/17/2021
Systems, Inc.	Platform				Log4Shell Vulnerability			
					in Apache Log4j			
Zerto					Zerto KB			
Zesty					Zesty Log4j Exploit			
Zimbra					BugZilla Zimbra			
Zix					Zix Appriver Statement			12/16/2021
Zoom					Zoom Security Exposure			
ZPE systems					ZpeSystems			
$\operatorname{Inc}$					CVE-2021-44228			
Zscaler	See Link		Not Affected	No	$CVE-2021-44228 \log 4j$			12/15/2021
	(Multiple				Vulnerability			
	Products)							
Zyxel					Zyxel Security Advisory			
					for Apache Log4j			
Zyxel	Security Firewall/Gatewa	ZLD Firmware Security sys Services, Nebula	Not Affected	N/A	Zyxel Security Advisory			12/14/2021