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

Status Descriptions

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

Software List

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

- Kevin Beaumont
- SwitHak

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
1Password 2n 3CX	1Password		Not affected		1Password public response on Reddit 2n Advisory Link 3CX Community			12/20/2021
3M Health Informa- tion Systems	CGS		Affected	Unknown	Thread Link CGS: Log4j Software Update(login required)	This advisory is available to customer only and has not been reviewed by CISA.		12/15/2021
7-Zip ABB ABB	ABB Remote Service	ABB Remote Platform (RAP)	Affected		7Zip Discussion Link ABB Link Details are shared with active subscribers			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
ABB	AlarmInsight	AlarmInsight	Under					
	Cloud	KPI Dashboards	Investigati	on				
		1.0.0						
ABB	B&R	See Vendor			BR-Automation			
	Products	Advisory			Advisory			
Abbott					Abbott Advisory			12/30/2021
					Link			
Abnormal	Abnormal		Not		Abnormal Blog			
Security	Security		affected					
Accellence					Accellence			
					Article			

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
ccellion	Kiteworks	v7.6 release	Fixed	Yes	Kiteworks	"As a	12/16/2021
					Statement	precau-	
						tion,	
						Kite-	
						works	
						re-	
						leased	
						a 7.6.1	
						Hotfix	
						soft-	
						ware	
						update	
						to	
						address	
						the	
						vulner-	
						ability.	
						This	
						patch	
						release	
						adds	
						the mit-	
						igation	
						for	
						CVE-	
						2021-	
						44228	
						con-	
						tained	
						in the	
						Solr	
						pack-	
						age as	
						recom-	
						mended	
						by	
						Apache	
						Solr	
						group.	
						Specifi-	
						cally, it	
						up-	
						dates	
						the	
						Log4j	
						library	
						to a	
						non-	
						vulnerable	
					3	version	
						on Cen-	
						tOS 7	
						sys-	
						tems as	
						well as	
						adds	
						the	
						recom-	
						mended	
						option	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Acquia					Acquia Article			
Acronis					Acronis Advisory			
					Link			
ctiveStat	e				ActiveState Blog			
					Post			
daptec					Adaptec Link			
ddigy					Addigy Blog Post			
deptia					Adeptia Article			
dobe					Adobe			
oldFusion	n				ColdFusion Link			
DP					ADP Alert Link			
FAS					AFAS Software			
oftware					Link			
FHCAN	AFHCANsu	iite8.0.7 - 8.4.3	Not		https://afhcan.			
Global			Affected		org/support.aspx			
LC					Ο ₁ 11 T			
AFHCAN	AFHCANSe	erv & :0.7 - 8.4.3	Not		https://afhcan.			
Global			Affected		org/support.aspx			
LC			111100004		org/ support traspir			
FHCAN	AFHCANca	art 8.0.7 - 8.4.3	Not		https://afhcan.			
Hobal	111 11 0111 100		Affected		org/support.aspx			
LC			Tinected		org/support.aspx			
FHCAN	AFHCANw	eb 8.0.7 - 8.4.3	Not		https://afhcan.			
Hobal	711 110711 W	CD 0.0.1 0.1.0	Affected		org/support.aspx			
LC			Tinecoca		org/support.aspx			
FHCAN	AFHCANm	obi 8 e0.7 - 8.4.3	Not		https://afhcan.			
Global	711 1107111111	0.4.0	Affected		org/support.aspx			
LC			Affected		org/support.aspx			
FHCAN	A FHC A Nun	pda& 0.7 - 8.4.3	Not		https://afhcan.			
Global	AFIIOANuj	puada.1 - 0.4.5	Affected		org/support.aspx			
LC			Anected		org/support.aspx			
gilysys					Agilysys Link			
dvanced	Active		Not	No	Log4J	This		12/14/2021
	MFT		Affected	INU	Log4J Vulnerabilty	advi-		14/2021
ystems	ML I		Affected		vumerabilty			
oncepts						sory is		
ormally						avail-		
scape)						able to		
						cus-		
						tomers		
						only		
						and has		
						not		
						been re-		
						viewed		
						by		
						CISA		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Advanced Systems Concepts (formally Jscape)	MFT Server		Not Affected	No	Log4J Vulnerabilty	This advisory is available to customers only and has not been reviewed by CISA		12/14/2021
Advanced Systems Concepts (formally Jscape)	MFT Gateway		Not Affected	No	Log4J Vulnerabilty	This advisory is available to customers only and has not been reviewed by CISA		12/14/2021
Advanced Systems Concepts (formally Jscape)	MFT		Not Affected	No	Log4J Vulnerabilty	This advisory is available to customers only and has not been reviewed by CISA		12/14/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Akamai	SIEM	All	Affected	Yes	Akamai SIEM	v1.4.11		12/15/2021
	Splunk				Integration	is the		, ,
	Connector				<u> </u>	new		
						recom-		
						menda-		
						tion for		
						mitiga-		
						tion of		
						log4j		
						vulnerab	ilities	
Alcatel					Alcatel Link			
Alertus					Alertus Article			
					Link			
Alexion					Alexion Blog			
					Post			
Alfresco					Alfresco Blog			
					Post			
AlienVault					AlienVault			
					Article Link			
Alphatron					Alphatron			
Medical					Medical Website			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
mazon	AWS	Linux 1,2	Not	No		Notes:	12/15/2021
			Affected			Ama-	
						zon	
						Linux 1	
						had	
						aws api-	
						tools	
						which	
						were	
						Java	
						based	
						but	
						these	
						were	
						depre-	
						cated	
						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-	
Amazon	AWS API	All	Fixed		Amazon AWS	gp2	12/20/2021
mazon	Gateway	All	rixeu				14/20/2021
	Gateway				Link		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Amazon	AWS CloudHSM	< 3.4.1.	Affected		Apache Log4j2 Security Bulletin (CVE-2021- 44228)			
Amazon	AWS Connect	All	Fixed		(amazon.com) Vendor Link	Vendors recom- mend evaluat- ing compo- nents of the envi- ron- ment outside of the Ama- zon Con- nect service bound- ary, which may require sepa- rate/add cus- tomer		12/23/2021
Amazon	AWS Lambda	Unknown	Affected	Yes	Apache Log4j2 Security Bulletin (CVE-2021- 44228) (amazon.com)	mitigatio	11	
Amazon	EC2	Amazon Linux 1 & 2	Not Affected		Apache Log4j2 Security Bulletin (CVE-2021- 44228) (amazon.com)			12/15/2021
Amazon	AWS DynamoDB	Unknown	Fixed		Update for Apache Log4j2 Issue (CVE-2021- 44228)			12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Amazon	AWS ElastiCache	Unknown	Fixed		Update for Apache Log4j2 Issue (CVE-2021- 44228)			12/17/2021
Amazon	AWS Inspector	Unknown	Fixed		Update for Apache Log4j2 Issue (CVE-2021- 44228)			12/17/2021
Amazon	AWS RDS	Unknown	Fixed		Update for Apache Log4j2 Issue (CVE-2021- 44228)	Amazon RDS and Ama- zon Aurora have been up- dated to miti- gate the issues identi- fied in CVE- 2021- 44228		12/17/2021
Amazon	AWS S3	Unknown	Fixed		Update for Apache Log4j2 Issue (CVE-2021- 44228)			12/14/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
endor mazon	Product AWS SNS	Version(s) Unknown	Status Fixed	Update Available	Vendor Link Update for Apache Log4j2 Issue (CVE-2021-44228)	Notes Amazon SNS sys- tems that serve cus- tomer traffic are patched against the Log4j2 issue. We are work- ing to apply the Log4j2 patch to sub- systems that operate sepa- rately from SNS's sys- tems that	Other References	Last Updated 12/14/2021
Λ mazon	AWS SQS	Unknown	Fixed		Update for Apache Log4j2 Issue (CVE-2021- 44228)	serve cus- tomer traffic		12/15/2021

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
nazon	AWS EKS,	Unknown	Affected	Yes	Update for	To help		12/16/2021
	ECS,				Apache Log4j2	miti-		
	Fargate				Issue (CVE-2021-	gate		
					44228)	the		
						impact		
						of the		
						open-		
						source		
					Apache			
					"Log4j2" utility			
					(CVE-			
						2021-		
						44228		
						and		
						CVE-		
						2021-		
						45046)		
						secu-		
						rity		
						issues		
						on cus-		
						tomers'		
						con-		
						tainers,		
						Ama-		
						zon		
						EKS,		
						Ama-		
						zon		
				ECS,				
						and		
						AWS		
						Fargate		
						are de-		
						ploying a		
						a Linux-		
						based		
						update		
						(hot-		
						patch).		
						This		
						hot-		
						patch		
						will		
						require		
						cus-		
						tomer		
					11	opt-in		
						to use,		
						and dis-		
						ables		
						JNDI		
						lookups		
						from		
						the		
						Log4J2		
						library		
						in cus-		

in cus-

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Amazon	AWS ELB	Unknown	Fixed		Update for Apache Log4j2 Issue (CVE-2021- 44228)			12/16/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Vendor Amazon	AWS Kinesis Data Stream	Version(s) Unknown	Affected	Yes Yes	Vendor Link Update for Apache Log4j2 Issue (CVE-2021-44228)	We are actively patching all subsystems that use Log4j2 by applying updates. The Kinesis Client Library (KCL) version 2.X and the Kinesis Producer Library (KPL) are not impacted. For customers	Other References	Last Updated 12/14/2021
						tomers using KCL 1.x, we have re- leased an up- dated		
						version and we strongly recom- mend that all KCL version		
					13	1.x customers upgrade to KCL version 1.14.5 (or		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Amazon	OpenSearch	Unknown	Affected	Yes	Apache Log4j2 Security Bulletin (CVE-2021- 44228) (amazon.com),			
	TD 1.		37.		(R20211203-P2)	a ·		
Amazon	Translate		Not affected		Amazon Translate	Service not identi- fied on AWS Log4j Secu- rity Bul- letin		
AMD	All		Not Affected		AMD Advisory Link	Currently no AMD prod- ucts have been identi- fied as af- fected. AMD is contin- uing its analysis.	7,	12/22/2021
Anaconda	Anaconda	4.10.3	Not Affected		https: //docs.conda.io/ projects/conda/ en/latest/index. html	anarysis.		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
pache	Product ActiveMQ Artemis	Version(s) All	Status Not Affected	Update Available Yes	Vendor Link ApacheMQ - Update on CVE-2021-4428	Notes Other References ActiveMQ Artemis does not use Log4j for logging. How- ever, Log4j 1.2.17 is in- cluded in the Hawtio- based web console applica- tion archive (i.e. web/ console. war/ WEB- INF/ lib). Al- though this version of Log4j is not im- pacted by CVE- 2021- 44228 future ver- sions of Artemis	Last Updated 12/21/2021
					15	will be up- dated so that the Log4j jar is no longer in- cluded in the web console applica- tion archive.	

See

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Apache	Airflow		Not affected		Apache Airflow	Airflow is written in Python		

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
ndor ache	Product Camel	Version(s) 3.14.1.3.11.5,3.7.7		Yes Yes	Vendor Link APACHE CAMEL AND CVE-2021-44228 (LOG4J)	Apache Camel does not directly depend on Log4j 2, so we are not af- fected by CVE- 2021- 44228.If you ex- plicitly added the Log4j 2 depen- dency to your own applica- tions, make sure to up- grade.Apache Camel does use log4j during testing itself, and there- fore you can find that we	Last Updated 12/13/2021
					17	have been using log4j v2.13.3 release in our latest LTS releases Camel 3.7.6,	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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)	10g4j.		12/13/2021
Apache	Camel 2		Not Affected	None	APACHE CAMEL AND CVE-2021-44228 (LOG4J)			12/13/2021
Apache	Druid	< druid 0.22.0	Affected	Yes	Release druid-0.22.1 · apache/druid · GitHub			12/12/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Vendor Apache	Flink	Version(s) < 1.14.2, 1.13.5, 1.12.7, 1.11.6	Status Fixed	Yes Yes	Vendor Link 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	Other References https://flink.apache.org/ news/2021/12/16/log4j- patch-releases.html	Last Updated 12/12/2021
					19	version up- grade for Log4j to		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Apache	Kafka	All	Not	No	Kafka Apache	The		12/14/2021
			Affected		List	current		
						DB		
						lists		
						Apache		
						Kafka		
						as im-		
						pacted.		
						Apache		
						Kafka		
						uses		
						Log4jv1,		
						not v2.		
Apache	Kafka	Unknown	Affected	No	Log4j – Apache	Only		
					Log4j Security	vulner-		
					Vulnerabilities	able in		
						certain		
						configura	tion(s)	
Apache	Log4j	< 2.15.0	Affected	Yes	Log4j – Apache			
					Log4j Security			
					Vulnerabilities			
Apache	Solr	7.4.0 to 7.7.3,	Fixed	Yes	Apache Solr	Update	Apache Solr 8.11.1	12/16/2021
		8.0.0 to 8.11.0			Security	to	downloads	
						8.11.1		
						or		
						apply		
						fixes as		
						de-		
						scribed		
					in Solr			
				secu-				
						rity		
						advisory		

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

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
ache	Tomcat	9.0.x	Not		Apache Tomcat	Apache		12/21/2021
			Affected		Security Notes	Tomcat		
			(See			9.0.x		
			Notes)			has no		
						depen-		
						dency		
						on any		
						version		
						of $log4j$.		
						Web		
						applica-		
						tions		
						de-		
						ployed		
						on		
						Apache		
						Tomcat		
						may		
						have a		
						depen-		
						dency		
						on		
						log4j.		
						You		
						should		
						seek		
						support		
						from		
						the		
						applica-		
						tion		
						vendor		
						in this in-		
						stance. It is		
						possi-		
						ble to		
						config-		
						ure		
						Apache		
						Tomcat		
						9.0.x to		
						use		
						log4j		
						2.x for		
						Tom-		
						cat's		
						inter-		
					00	nal		
					22	logging.		
						This re-		
						quires		
						explicit		
						configu-		
						ration		
						and the		
						addi-		
						tion of		
						the		

the

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 · open- cast/opencast · GitHub			
Performance Ltd	n DBMarlin	Not Affected		Common Vulnerabilities Apache log4j Vulnerability CVE-2021-4428	Animaa Tinla			12/15/2021
Apigee Apollo					Apigee Link Apollo Community Link			
Appdynan	nics				Appdynamics Advisory Link			
Appeon	PowerBuilder	PowerBuilder 2017-2021 regardless of product edition	Affected	No				12/15/2021
AppGate		product cartion			AppGate Blog Post			
Appian	Appian Platform	All	Fixed		KB-2204 Information about the Log4j2 security vulnerabilities (CVE-2021- 44228 & CVE-2021- 45046)			12/22/2021
Applicatio Perfor- mance Ltd	n DBMarlin		Not Affected		Common Vulnerabilities Apache log4j Vulnerability CVE-2021-4428			12/15/2021
APPSHEE	ET				APPSHEET Community Link			
Aptible	Aptible	ElasticSearch 5.x	Affected	Yes	Aptible Status - Log4j security incident CVE-2021-27135			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Update
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	Mitigatio instructions to remove the affected class.	n	12/15/2021
APC by Schneider Electric	Powerchute Network Shutdown	4.2, 4.3, 4.4, 4.4.1		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 Doc	Mitigation instructions to remove the affected class.	n	12/15/2021
Arbiter Systems Arca Noae	All		Not Affected		Arbiter Systems Advisory Link Arca Noae Link			12/22/2021
Arcserve	Arcserve Backup	All	Not Affected	No	https://support. storagecraft. com/s/article/ Log4J-Update		https://support.storagecraft.com/s/question/ 0D51R000089NnT3SAK/ does-storagecraft-have-a- publicly-available- response-to-the-log4j- vulnerability-is-there-a- reference-for-any-findings- negative-positive-the- company-has-in-their- investigations-it-seems-it- would-greatly-benefit- support-and-customers- both?language=en_US	12/14/2021

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

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References Last Updated
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 vul- nerable to remote code ex- ecution but may leak infor- mation due to the bun- dled Elastic- search component being
Atlassian	Confluence Server & Data Center	All	Not Affected		Multiple Products Security Advisory - Log4j Vulnerable To Remote Code Execution - CVE-2021-44228	vulnerable. This product may be af- fected by a related but lower severity vulner- ability if run- ning in a specific non- default configuration.

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Atlassian	Crowd Server & Data Center	All	Not Affected		Multiple Products Security Advisory - Log4j Vulnerable To Remote Code Execution - CVE-2021-44228	This product may be affected by a related but lower severity vulnerability if running in a specific nondefault		
Atlassian	Crucible	All	Not Affected		Multiple Products Security Advisory - Log4j Vulnerable To Remote Code Execution - CVE-2021-44228	configura This prod- uct may be af- fected by a related but lower severity vulner- ability if run- ning in a specific non- default configura		

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

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
todesk			Under		Autodesk Article	Autodes	k	12/21/2021
			Investigat	ion	Link	is con-		
						tinuing		
						to per-		
						form a		
						thor-		
						ough		
						investi-		
						$_{ m in}$		
						relation		
						to the		
						re-		
						cently		
						discov-		
						ered		
						Apache		
						Log4j		
						secu-		
						rity		
						vulner-		
						abili-		
						ties.		
						We con-		
						tinue to		
						imple-		
						ment several		
						mitigat-		
						ing		
						factors		
						for our		
						prod-		
						ucts		
						includ-		
						ing		
						patch-		
						ing,		
						net-		
						work		
						firewall		
						blocks,		
						and up-		
						dated		
						detec-		
						tion		
						signa- tures to		
						reduce		
						the		
					31	threat		
						of this		
						vulner-		
						ability		
						and en-		
						hance		
						our		
						ability		
						to		
						anickly		

quickly

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Automox					Automox Blog			
					Post			
Autopsy					Autopsy Link			
Auvik					Auvik Status			
					Link			
Avantra					Avantra			
SYSLINK					SYSLINK Article			
Avaya	Avaya	3.5, 3.6, 3.6.1,	Affected	No	Apache Log4J			12/14/2021
	Analytics	3.7, 4			Vulnerability -			, ,
					Impact for Avaya			
					products Avaya			
					Product Security			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Avaya	Avaya Aura® Application Enablement Services	8.1.3.2, 8.1.3.3, 10.1	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security		PSN020551u	12/14/2021
Avaya	Avaya Aura® Contact Center	7.0.2, 7.0.3, 7.1, 7.1.1, 7.1.2	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Avaya Aura® Device Services	8, 8.1, 8.1.4, 8.1.5	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Avaya Aura® Media Server	8.0.0, 8.0.1, 8.0.2	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security		PSN020549u	12/14/2021
Avaya	Avaya Aura® Presence Services	10.1, 7.1.2, 8, 8.0.1, 8.0.2, 8.1, 8.1.1, 8.1.2, 8.1.3, 8.1.4	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Avaya Aura® Session Manager	10.1, 7.1.3, 8, 8.0.1, 8.1, 8.1.1, 8.1.2, 8.1.3	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security		PSN020550u	12/14/2021
Avaya	Avaya Aura® System Manager	10.1, 8.1.3	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security		PSN005565u	12/14/2021
Avaya	Avaya Aura® Web Gateway	3.11[P], 3.8.1[P], 3.8[P], 3.9.1 [P], 3.9[P]	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021
Avaya	Avaya Breeze TM	3.7, 3.8, 3.8.1	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security			12/14/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link Notes	Other References	Last Updated
Avaya	Avaya Contact Center Select	7.0.2, 7.0.3, 7.1, 7.1.1, 7.1.2	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security		12/14/2021
Avaya	Avaya CRM Connector - Connected Desktop	2.2	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security		12/14/2021
Avaya	Avaya Device Enablement Service	3.1.22	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security		12/14/2021
Avaya	Avaya Meetings	9.1.10, 9.1.11, 9.1.12	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security		12/14/2021
Avaya	Avaya one cloud private -UCaaS - Mid Market Aura	1	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security		12/14/2021
Avaya	Avaya OneCloud- Private	2	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security		12/14/2021
Avaya	Avaya Session Border Controller for Enterprise	8.0.1, 8.1, 8.1.1, 8.1.2, 8.1.3	Affected	Yes	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security	PSN020554u	12/14/2021
Avaya	Avaya Social Media Hub		Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security		12/14/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link Notes Other Reference	es Last Updated
Avaya	Avaya Workforce Engagement	5.3	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya	12/14/2021
Avaya	Business Rules Engine	3.4, 3.5, 3.6, 3.7	Affected	No	Product Security Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security	12/14/2021
Avaya	Callback Assist	5, 5.0.1	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya	12/14/2021
Avaya	Control Manager	9.0.2, 9.0.2.1	Affected	No	Product Security Apache Log4J Vulnerability - Impact for Avaya products Avaya	12/14/2021
Avaya	Device Enrollment Service	3.1	Affected	No	Product Security Apache Log4J Vulnerability - Impact for Avaya products Avaya	12/14/2021
Avaya	Equinox TM Conferencing	9.1.2	Affected	No	Product Security Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security	12/14/2021
Avaya	Interaction Center	7.3.9	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security	12/14/2021
Avaya	IP Office TM Platform	11.0.4, 11.1, 11.1.1, 11.1.2	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security	12/14/2021
Avaya	Proactive Outreach Manager	3.1.2, 3.1.3, 4, 4.0.1	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya Product Security	12/14/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Avaya	Avaya Aura® Device Services	8.0.1, 8.0.2, 8.1.3	Affected	No	Apache Log4J Vulnerability - Impact for Avaya products Avaya			12/14/2021
AVEPOIN	Т				Product Security AVEPOINT			
AVM					Notification AVM Link			
AvTech					AvTech			
RoomAlert	t				RoomAlert			
ATTO					Article			
AWS New					AWS New Security Bulletin			
AXON					AXON Link			
AXS					AXS Guard Blog			
Guard					Post			
Axways Application	ng				Axways Applications			
пррисано	115				Link			
B&R In-	APROL		Not		B&R Statement			12/16/2021
dustrial Automatio			Affected					
Baxter	11			Under Investigation	Baxter Advisory			12/20/2021
				2 and Garage	Link			, -, -
BackBox					BackBox Update			
Balbix Baramund	:				Balbix Blog Post Baramundi			
Products	1				Products Forum			
Barco					Barco Link			
Barracuda			37 .	27	Barracuda Link			12/20/2021
BBraun	Outlook® Safety		Not Affected	No	BBraun Advisory Link			12/20/2021
	Infusion		Affected		Lillik			
	System							
	Pump							
BBraun	family Space®		Not	No	BBraun Advisory			12/20/2021
DDIaun	Infusion		Affected	110	Link			12/20/2021
	Pump							
	family (In-							
	fusomat® Space®							
	Infusion							
	Pump,							
	Perfusor®							
	Space® Infusion							
	musion							

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
BBraun	Pump, SpaceSta- tion, and Space® Wireless		Not Affected	No	BBraun Advisory Link			12/20/2021
BBraun	Battery) DoseTrac® Server, DoseLink TM Server, and Space® Online Suite		Not Affected	No	BBraun Advisory Link			12/20/2021
DD	Server software		N-4	N.	DD Advisor			19 /90 /9091
BBraun	Pinnacle® Compounder		Not Affected	No	BBraun Advisory Link			12/20/2021
BBraun	APEX® Compounder		Not Affected	No	BBraun Advisory Link			12/20/2021
BD	Arctic Sun TM 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 Health- Sight TM Clinical Advisor		Not Affected	No	BD Advisory Link			12/20/2021
BD	BD Health- Sight TM Data Manager		Not Affected	No	BD Advisory Link			12/20/2021
BD	BD Health- Sight TM Diversion Management		Not Affected	No	BD Advisory Link			12/20/2021
BD	BD Health- Sight TM Infection Advisor		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 Health-Sight TM Inventory Optimization Analytics		Not Affected	No	BD Advisory Link			12/20/2021
BD	BD Health- Sight TM Medication Safety		Not Affected	No	BD Advisory Link			12/20/2021
BD	BD Knowledge Portal for Infusion Technologies		Not Affected	No	BD Advisory Link			12/20/2021
BD	BD Knowledge Portal for Medication Technologies		Not Affected	No	BD Advisory Link			12/20/2021
BD	BD Knowledge Portal for BD Pyxis TM Supply		Not Affected	No	BD Advisory Link			12/20/2021
BD	BD Synapsys TM Informatics Solution		Not Affected	No	BD Advisory Link			12/20/2021
BD	BD Veritor TM COVID At Home Solution Cloud		Not Affected	No	BD Advisory Link			12/20/2021
Beckman			Under		Beckman Coulte	r		12/20/2021
Coulter			Investigati	on	Advisory Link			42/22/22
Beijer Electronics	acirro+		Not Affected		Beijer Electronic Advisory Link	S		12/22/2021
Beijer Electronics	BFI		Not Affected		Beijer Electronic Advisory Link	S		12/22/2021
Beijer	BSD servo		Not		Beijer Electronic	S		12/22/2021
Electronics Beijer Electronics	drives CloudVPN		Affected Not Affected		Advisory Link Beijer Electronic Advisory Link			12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Beijer Electronics	FnIO-G and M Distributed IO		Not Affected		Beijer Electronics Advisory Link			12/22/2021
Beijer Electronics	iX Developer		Not Affected		Beijer Electronics Advisory Link			12/22/2021
Beijer Electronics	Nexto		Not Affected		Beijer Electronics Advisory Link			12/22/2021
Beijer Electronics	Nexto Xpress compact controller		Not Affected		Beijer Electronics Advisory Link			12/22/2021
Beijer Electronics	WARP Engineering Studio		Not Affected		Beijer Electronics Advisory Link			12/22/2021
Bender Best Practical Request Tracker (RT) and Request Tracker for Incident Response (RTIR)			Under Investigation		BioMerieux Advisory Link Bender Link Vendor Link			12/22/2021
BeyondTrus	Manage- ment Cloud	Unknown	Fixed	Yes	Security Advisory – Apache Log4j2 CVE 2021-44228 (Log4Shell)			2021-12-17
BeyondTrus	stPrivilege Manage- ment Reporting in BeyondInsigl	21.2	Fixed	Yes	Security Advisory – Apache Log4j2 CVE 2021-44228 (Log4Shell)			2021-12-17
BeyondTrus		Unknown	Not Affected		Security Advisory – Apache Log4j2 CVE 2021-44228 (Log4Shell)			2021-12-17

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
BeyondTr	rust				BeyondTrust			
Bomgar					Bomgar Link			
BisectHos	sting				BisectHosting			
	0				Link			
BitDefend	ler				BitDefender			
					Advisory Link			
BitNami					BitNami By			
Ву					VMware			
VMware					VIVIWAIC			
BitRise					BitRise Post			
Bitwarder			Not		Bitwarden			
Ditwarder	1		Affected		Community Link			
Biztory	Fivetran		Not		Apache Log4j2		Vendor review indicated	
Diztory	rivetian		Affected		Vulnerability -		Fivetran is not vulnerable	
			Affected					
					Updates For		to Log4j2	
D1 1					Biztory Clients			
Black					Black Kite Link			
Kite					D1 G			
Blancco					Blancco Support			
					Link			
Blumira					Blumira Link			
BMC	Bladelogic		Under		BMC Security			
	Database		Investigat	on	Advisory for			
	Automation				CVE-2021-44228			
					Log4Shell			
					Vulnerability -			
					Blogs &			
					Documents -			
					BMC			
					Community			
BMC	BMC AMI		Under		BMC Security			
	Ops		Investigat	on	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 AMI		Under		BMC Security			
	Products		Investigati	on	Advisory for			
					CVE-2021-44228			
					Log4Shell Vulnerability -			
					Blogs &			
					Documents -			
					BMC			
					Community			
BMC	BMC		Under		BMC Security			
	Compuware		Investigati	on	Advisory for			
					CVE-2021-44228			
					Log4Shell			
					Vulnerability -			
					Blogs &			
					Documents -			
					BMC			
DMC	BMC Helix		Under		Community			
BMC	Automa-		Investigation	on	BMC Security Advisory for			
	tion		mvestigati	OII	CVE-2021-44228			
	Console				Log4Shell			
	Colligore				Vulnerability -			
					Blogs &			
					Documents -			
					BMC			
					Community			
BMC	BMC Helix		Under		BMC Security			
	Business		Investigati	on	Advisory for			
	Workflows				CVE-2021-44228			
					Log4Shell			
					Vulnerability -			
					Blogs &			
					Documents - BMC			
					Community			
BMC	BMC		Under		BMC Security			
DIVIO	Helix Client		Investigati	on	Advisory for			
	Management		111105018401		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			
	Cloud Cost		Investigation	on	Advisory for			
					CVE-2021-44228			
					Log4Shell			
					Vulnerability -			
					Blogs &			
					Documents -			
					BMC			
					Community			
BMC	BMC Helix		Under		BMC Security			
	Cloud		Investigation	on	Advisory for			
	Security				CVE-2021-44228			
					Log4Shell			
					Vulnerability -			
					Blogs &			
					Documents -			
					BMC			
DMC	DMC II I		TT 1		Community			
BMC	BMC Helix		Under		BMC Security			
	CMDB		Investigation	on	Advisory for			
					CVE-2021-44228			
					Log4Shell Vulnerability -			
					Blogs &			
					Documents -			
					BMC			
					Community			
BMC	BMC Helix		Under		BMC Security			
DIVIO	Continuous		Investigation	an	Advisory for			
	Optimization		Investigati	<i>7</i> 11	CVE-2021-44228			
	Optimization	1			Log4Shell			
					Vulnerability -			
					Blogs &			
					Documents -			
					BMC			
					Community			
BMC	BMC Helix		Under		BMC Security			
	Control-M		Investigation	on	Advisory for			
					CVE-2021-44228			
					Log4Shell			
					Vulnerability -			
					Blogs &			
					Documents -			
					BMC			
					Community			

Vendor	Product Version(s)	Status Update Available	Vendor Link Not	es Other References	Last Updated
BMC	BMC Helix Digital Workplace	Under Investigation	BMC Security Advisory for CVE-2021-44228		
			Log4Shell Vulnerability -		
			Blogs &		
			Documents -		
			BMC		
BMC	BMC Helix	Under	Community BMC Security		
DMC	Discovery	Investigation	Advisory for		
	V	0	CVE-2021-44228		
			Log4Shell		
			Vulnerability - Blogs &		
			Documents -		
			BMC		
DIG	DIG II II	TT 1	Community		
BMC	BMC Helix ITSM	Under Investigation	BMC Security Advisory for		
	110111	mvestigation	CVE-2021-44228		
			Log4Shell		
			Vulnerability -		
			Blogs & Documents -		
			BMC		
			Community		
BMC	BMC Helix	Under	BMC Security		
	Knowledge	Investigation	Advisory for		
	Management		CVE-2021-44228 Log4Shell		
			Vulnerability -		
			Blogs &		
			Documents -		
			BMC Community		
BMC	BMC Helix	Under	BMC Security		
	Operations	Investigation	Advisory for		
	Manage-		CVE-2021-44228		
	ment with AIOps		Log4Shell Vulnerability -		
	торь		Blogs &		
			Documents -		
			BMC		
			Community		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
BMC	BMC Helix Platform		Under Investigation	an.	BMC Security Advisory for			
	Platform		mvestigatio	011	CVE-2021-44228			
					Log4Shell			
					Vulnerability -			
					Blogs &			
					Documents -			
					BMC			
					Community			
BMC	BMC Helix		Under		BMC Security			
	platform		Investigation	on	Advisory for			
	1		O		CVE-2021-44228			
					Log4Shell			
					Vulnerability -			
					Blogs &			
					Documents -			
					BMC			
					Community			
BMC	BMC Helix		Under		BMC Security			
	Remediate		Investigation	on	Advisory for			
					CVE-2021-44228			
					Log4Shell			
					Vulnerability -			
					Blogs &			
					Documents -			
					BMC			
DMC	BMC Helix		II J		Community			
BMC	Remediate		Under	2.00	BMC Security Advisory for			
	пешешате		Investigation	011	CVE-2021-44228			
					Log4Shell			
					Vulnerability -			
					Blogs &			
					Documents -			
					BMC			
					Community			
BMC	BMC Helix		Under		BMC Security			
	Remedyforce	,	Investigation	on	Advisory for			
	•				CVE-2021-44228			
					Log4Shell			
					Vulnerability -			
					Blogs &			
					Documents -			
					BMC			
					Community			

Vendor	Product Version	on(s) Status Update Available	Vendor Link	Notes	Other References	Last Updated
BMC	BMC Helix Virtual Agent	Under Investigation	BMC Security Advisory for CVE-2021-44228			
			Log4Shell Vulnerability -			
			Blogs &			
			Documents -			
			BMC Community			
BMC	Cloud	Under	BMC Security			
Divic	Lifecycle	Investigation	Advisory for			
	Management	<u> </u>	CVE-2021-44228			
			Log4Shell			
			Vulnerability - Blogs &			
			Documents -			
			BMC			
			Community			
BMC	Control-M	Under	BMC Security			
		Investigation	Advisory for CVE-2021-44228			
			Log4Shell			
			Vulnerability -			
			Blogs &			
			Documents - BMC			
			Community			
BMC	Footprints	Under	BMC Security			
		Investigation	Advisory for			
			CVE-2021-44228			
			Log4Shell Vulnerability -			
			Blogs &			
			Documents -			
			BMC			
BMC	MainView	Under	Community BMC Security			
DMC	Middle-	Investigation	BMC Security Advisory for			
	ware	111,000,900,011	CVE-2021-44228			
	Administrator		Log4Shell			
			Vulnerability -			
			Blogs & Documents -			
			BMC			
			Community			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
BMC	MainView Middle- ware Monitor		Under Investigation	on	BMC Security Advisory for CVE-2021-44228			
	Monitor				Log4Shell Vulnerability - Blogs &			
					Documents - BMC			
D) (G	.				Community			
BMC	Remedy		Under		BMC Security			
	ITSM (IT Service		Investigation	on	Advisory for CVE-2021-44228			
	Management)				Log4Shell Vulnerability -			
					Blogs &			
					Documents -			
					BMC			
					Community			
BMC	SmartIT		Under		BMC Security			
			Investigation	on	Advisory for			
					CVE-2021-44228			
					Log4Shell			
					Vulnerability - Blogs &			
					Documents -			
					BMC			
					Community			
BMC	Track-It!		Under		BMC Security			
			Investigation	on	Advisory for			
					CVE-2021-44228			
					Log4Shell			
					Vulnerability -			
					Blogs & Documents -			
					BMC			
					Community			
BMC	TrueSight		Under		BMC Security			
	Automa-		Investigation	on	Advisory for			
	tion for				CVE-2021-44228			
	Networks				Log4Shell			
					Vulnerability -			
					Blogs &			
					Documents - BMC			
					Community			
					Community			

Vendor	Product Version(s)	Status Update Available	Vendor Link Nor	tes Other References	Last Updated
BMC	TrueSight Automa- tion for	Under Investigation	BMC Security Advisory for CVE-2021-44228		
	Servers		Log4Shell		
	Servers		Vulnerability -		
			Blogs &		
			Documents -		
			BMC		
DMC	TD C: 1	TT 1	Community		
BMC	TrueSight Capacity	Under Investigation	BMC Security Advisory for		
	Optimization	Investigation	CVE-2021-44228		
	Optimization		Log4Shell		
			Vulnerability -		
			Blogs &		
			Documents - BMC		
			Community		
BMC	TrueSight	Under	BMC Security		
	Infrastruc-	Investigation	Advisory for		
	ture		CVE-2021-44228		
	Management		Log4Shell		
			Vulnerability -		
			Blogs &		
			Documents - BMC		
			Community		
BMC	TrueSight	Under	BMC Security		
21.10	Operations	Investigation	Advisory for		
	Management	Ŭ	CVE-2021-44228		
	-		Log4Shell		
			Vulnerability -		
			Blogs &		
			Documents -		
			BMC		
BMC	TrueSight	Under	Community BMC Security		
DMC	Orchestration	Investigation	Advisory for		
	Orchestration	mvestigation	CVE-2021-44228		
			Log4Shell		
			Vulnerability -		
			Blogs &		
			Documents -		
			BMC		
_			Community		
Boston		Under	Boston Scientific		12/20/2021
Scientific		Investigation	Advisory Link		

Vendor	Product Version(s)	Status Update Available	Vendor Link	Notes C	ther References	Last Updated
Bosch		Affected No	Bosch Advisory			12/22/2021
D			Link			
Box			Box Blog Post			
Brainworks			Brainworks Link			
BrightSign			BrightSign Link			
Broadcom	Advanced	Under	Broadcom			
	Secure	Investigation	Support Portal			
	Gateway					
_	(ASG)					
Broadcom	Automic		Broadcome			
	Automation		Automic			
			Automation Link			
Broadcom	BCAAA	Under	Broadcom			
		Investigation	Support Portal			
Broadcom	CA 9.1	Affected				
	Advanced					
	Authentication					
Broadcom	CA Risk	Affected				
	Authentication					
Broadcom	CA Strong	Affected				
	Authentication					
Broadcom	Cloud	Under	Broadcom			
	Workload	Investigation	Support Portal			
	Protection					
	(CWP)					
Broadcom	Cloud	Under	Broadcom			
	Workload	Investigation	Support Portal			
	Protection					
	for Storage					
	(CWP:S)					
Broadcom	CloudSOC	Not	Broadcom			
	Cloud	Affected	Support Portal			
	Access					
	Security					
	Broker					
	(CASB)					
Broadcom	Content	Under	Broadcom			
	Analysis	Investigation	Support Portal			
	(CA)					
Broadcom	Critical	Under	Broadcom			
	System	Investigation	Support Portal			
	Protection	-				
	(CSP)					
Broadcom	Data	Not	Broadcom			
	Center	Affected	Support Portal			
	Security		11			
	(DCS)					

Vendor	Product Version	(s) Status Update Available	Vendor Link	Notes	Other References	Last Updated
Broadcom	Data Loss	Not	Broadcom			
	Prevention	Affected	Support Portal			
	(DLP)					
Broadcom	Email	Under	Broadcom			
	Security	Investigation	Support Portal			
	Service					
D J	(ESS)	Not	D J			
Broadcom	Ghost Solution	Not Affected	Broadcom Support Portal			
	Suite	Affected	Support Fortai			
	(GSS)					
Broadcom	HSM	Under	Broadcom			
Droadcom	Agent	Investigation	Support Portal			
Broadcom	Industrial	Under	Broadcom			
	Control	Investigation	Support Portal			
	System	0	11			
	Protection					
	(ICSP)					
Broadcom	Integrated	Under	Broadcom			
	Cyber	Investigation	Support Portal			
	Defense					
	Manager					
	(ICDm)					
Broadcom	Integrated	Under	Broadcom			
	Secure	Investigation	Support Portal			
	Gateway					
D 1	(ISG)	27.	D 1			
Broadcom	IT Manage-	Not	Broadcom			
	ment	Affected	Support Portal			
Broadcom	Suite Layer7 API	Under	Broadcom			
Dioadcolli	Developer Developer	Investigation	Support Portal			
	Portal	mvestigation	Support 1 ortar			
Broadcom	Layer7 API	Not	Broadcom			
Broadcom	Gateway	Affected	Support Portal			
Broadcom		Not	Broadcom			
	Mobile API	Affected	Support Portal			
	Gateway					
Broadcom	Management	Under	Broadcom			
	Center	Investigation	Support Portal			
	(MC)					
Broadcom	PacketShaper	Under	Broadcom			
	(PS)	Investigation	Support Portal			
_	S-Series					
Broadcom	PolicyCenter	Under	Broadcom			
	(PC)	Investigation	Support Portal			
	S-Series					

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Broadcom	Privileged		Under		Broadcom			
	Access		Investigati	on	Support Portal			
	Manager							
Broadcom	Privileged		Under		Broadcom			
	Access		Investigati	on	Support Portal			
	Manager							
	Server							
	Control							
Broadcom	Privileged		Under		Broadcom			
	Identity		Investigati	on	Support Portal			
	Manager		O .		• •			
Broadcom	ProxySG		Not		Broadcom			
	v		Affected		Support Portal			
Broadcom	Reporter		Under		Broadcom			
	1		Investigati	on	Support Portal			
Broadcom	Secure		Under		Broadcom			
	Access		Investigati	on	Support Portal			
	Cloud		0		11			
	(SAC)							
Broadcom	Security		Not		Broadcom			
	Analytics		Affected		Support Portal			
	(SA)							
Broadcom	SiteMinder		Under		Broadcom			
	(CA Single		Investigati	on	Support Portal			
	Sign-On)		O .		• •			
Broadcom	SSL		Under		Broadcom			
	Visibility		Investigati	on	Support Portal			
	(SSLV)		O .		• •			
Broadcom	Symantec		Not		Broadcom			
	Control		Affected		Support Portal			
	Compli-				• •			
	ance Suite							
	(CCS)							
Broadcom	Symantec		Not		Broadcom			
	Directory		Affected		Support Portal			
Broadcom	·		Under		Broadcom			
	Endpoint		Investigati	on	Support Portal			
	Detection		.					
	and							
	Response							
	(EDR)							
Broadcom	Symantec		Under		Broadcom			
	Endpoint		Investigati	on	Support Portal			
	Encryption							
	(SEE)							

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Broadcom	Symantec Endpoint Protection (SEP)		Under Investigati	on	Broadcom Support Portal			
Broadcom	Symantec Endpoint Protection (SEP) for Mobile		Under Investigati	on	Broadcom Support Portal			
Broadcom	Symantec Endpoint Protection Manager (SEPM)	14.3	Affected	No	Broadcom Support Portal			
Broadcom	Symantec Identity Governance and Administration (IGA)		Not Affected		Broadcom Support Portal			
Broadcom	Symantec Mail Security for Microsoft Exchange (SMSMSE)		Under Investigati	on	Broadcom Support Portal			
Broadcom	Symantec Messaging Gateway (SMG)		Under Investigati	on	Broadcom Support Portal			
Broadcom	Symantec PGP Solutions		Not Affected		Broadcom Support Portal			
Broadcom	Symantec Protection Engine (SPE)		Under Investigati	on	Broadcom Support Portal			
Broadcom	Symantec Protection for SharePoint Servers (SPSS)		Under Investigati	on	Broadcom Support Portal			
Broadcom	VIP		Not Affected		Broadcom Support Portal			

Vendor	Product	Version(s)	Status Update Available	Vendor Link	Notes	Other References	Last Updated
Broadcom	VIP		Under	Broadcom			
	Authentica-		Investigation	Support Portal			
	tion						
	Hub						
Broadcom			Under	Broadcom			
	Isolation		Investigation	Support Portal			
D 1	(WI)		TT 1	D 1			
Broadcom			Under	Broadcom			
	Security Service		Investigation	Support Portal			
	(WSS)						
Broadcom			Under	Broadcom			
Droadcom	Webi dise		Investigation	Support Portal			
C4b				C4b XPHONE			
XPHONE				Link			
Camunda				Camunda Forum			
				Link			
Canary	All		Not	Canary Labs			12/22/2021
Labs			Affected	Advisory Link			
Canon	CT		Not	Canon Advisory			12/22/2021
	Medical		Affected	Link			
	Imaging						
-	Products						
Canon	MR		Not	Canon Advisory			12/22/2021
	Medical		Affected	Link			
	Imaging						
Canan	Products UL Medical		Not	Canan Advisan			19 /99 /9091
Canon	Imaging		Affected	Canon Advisory Link			12/22/2021
	Products		Affected	LIIIK			
Canon	XR		Not	Canon Advisory			12/22/2021
Canon	Medical		Affected	Link			12/22/2021
	Imaging		IIIootod	Ziiiii			
	Products						
Canon	NM		Not	Canon Advisory			12/22/2021
	Medical		Affected	Link			, ,
	Imaging						
	Products						
Canon	Vitrea		Under	Canon Advisory			12/22/2021
	Advanced		Investigation	Link			
	7.x						, .
Canon	Infinix-i		Under	Canon Advisory			12/22/2021
	(Angio		Investigation	Link			
a	Workstation)		0 11.			10/00/0001
Canon	Alphenix		Under	Canon Advisory			12/22/2021
	(Angio	\	Investigation	Link			
	Workstation)					

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
CapStorm	Copystorm		Under					12/22/2021
			Investigat	ion	~			
CarbonBla	ıck				CarbonBlack			
Canastraan	,		Not		Advisory Carestream			12/20/2021
Carestrean	n		Affected		Advisory Link			12/20/2021
CAS			Affected		CAS			
genesisWor	rld				genesisWorld			
50110010 1101					Link			
Cato					Cato Networks			
Networks					Blog Post			
Cepheid	C360		Not		Cepheid			12/20/2021
			Affected		Advisory Link			
Cepheid	GeneXpert		Under		Cepheid			12/20/2021
			Investigat	ion	Advisory Link			
Cerberus					Cerberus Article			
FTP	1: · · · NT A/TD	A 11	NT /		A C1 1			
Chaser	discrimiNAT Firewall	All	Not Affected		Are Chaser's			
Systems Check	CloudGuard	A 11	Not		products affected sk176865			
Point	CloudGuard	All	Affected		SK170005			
Check	Harmony	All	Not		sk176865			
Point	Endpoint		Affected					
	& Harmony							
	Mobile							
Check	Infinity		Not		sk176865			
Point	Portal		Affected					
Check	Quantum	All	Not		sk176865			
Point	Security		Affected					
C1 1	Gateway	A 11	37 .		1.150005	****		
Check	Quantum	All	Not		sk176865	Where		
Point	Security Management		Affected			used, uses the		
	Management					1.8.0_u		
						version	241	
						of the		
						JRE		
						that		
						pro-		
						tects		
						against		
						this		
						attack		
						by		
C1 1	CMD	A 11	NT :		1.150005	default.		
Check	SMB	All	Not		sk176865			
Point			Affected					

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Check	ThreatCloud		Not		sk176865			
Point			Affected		Cl. LLCC D			
CheckMK	1				CheckMK Forum			
Ciphermail	I				Ciphermail Blog			
OTO					Post			
CIS					CIS Customer			
C)	4 D .		A (C) 1	37	Portal			
Cisco	AppDynamic	es	Affected	Yes	Vulnerability in			
					Apache Log4j			
					Library Affecting			
					Cisco Products:			
O:	O:		II J		December 2021			
Cisco	Cisco		Under		Vulnerability in			
	Common		Investigat	ion	Apache Log4j			
	Services Platform				Library Affecting			
					Cisco Products: December 2021			
C:	Collector		A (C 4 - 3	No				
Cisco	Cisco Network		Affected	INO	Vulnerability in Apache Log4j			
	Services Or-				1 0 0			
	chestrator				Library Affecting Cisco Products:			
	(NSO)				December 2021			
Cisco	Cisco		Under		Vulnerability in			
Cisco	System Ar-		Investigat	ion	Apache Log4j			
	chitecture		Investigat	1011	Library Affecting			
	Evolution				Cisco Products:			
	Gateway				December 2021			
	(SAEGW)				December 2021			
Cisco	Cisco ACI		Under		Vulnerability in			
CIBCO	Multi-Site		Investigat	ion	Apache Log4j			
	Orchestrator		11110001800		Library Affecting			
	0101105010001				Cisco Products:			
					December 2021			
Cisco	Cisco ACI		Under		Vulnerability in			
	Virtual		Investigat	ion	Apache Log4j			
	Edge		O		Library Affecting			
	O				Cisco Products:			
					December 2021			
Cisco	Cisco		Under		Vulnerability in			
	Adaptive		Investigat	ion	Apache Log4j			
	Security		9		Library Affecting			
	Appliance				Cisco Products:			
	(ASA)				December 2021			
	Software							

Advanced Web Security Reporting Application isco Cisco AMP Virtual Private Cloud Applicate Clo	/endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Web Library Affecting Security Cisco Products: December 2021	Cisco	Cisco		Affected	No	Vulnerability in			
Security Reporting Application Cisco AMP Virtual Investigation Apaliance Councet Secure Mobility Client Because Cisco Appliance Secure Mobility Client Cloud Cisco Products: Secure Mobility Client December 2021 Library Affecting Cisco Products: Secure Mobility Client December 2021 Library Affecting Cisco Products: Cisco Products: Secure Mobility Client December 2021 Library Affecting Cisco Products: December 2021 Library Affecting Cisco Products: Cisco Produ		Advanced				Apache Log4j			
Reporting		Web				Library Affecting			
Application Sieco Cisco AMP		Security				Cisco Products:			
Sec		Reporting				December 2021			
Sec		Application							
Virtual	Cisco			Under		Vulnerability in			
Private Cloud Cisco Products: Cisco Products: Cisco Products: December 2021		Virtual		Investigat	on				
Cloud				Ö					
Appliance Cisco Any-						· ·			
iseo Cisco Any- Comect Investigation Apache Log4j Secure Mobility Client December 2021 isco Cisco Application Investigation Apache Log4j Policy Infrastructure Controller (APIC) Secure South Investigation Apache Log4j South Sout									
Comect Secure Library Affecting Secure Cisco Application Divestigation Cisco Products: Client December 2021 Sco Application Investigation Apache Log4j Policy Library Affecting Infrastructure Controller (APIC) Sco Cisco ASR Under Vulnerability in Footers Investigation Apache Log4j Routers Cisco Products: December 2021 Sco Cisco SSR Under Vulnerability in Footers December 2021 Sco Cisco Products: December 2021 Sco Cisco Under Vulnerability in Broadcloud Investigation Apache Log4j Calling Cisco Products: December 2021 Sco Cisco Under Vulnerability in Broadcloud Investigation Apache Log4j Cisco Products: December 2021 Sco Cisco Under Vulnerability in Broadcloud Investigation Apache Log4j Cisco Products: December 2021 Sco Cisco Under Vulnerability in BroadWorks Investigation Apache Log4j Cisco Products: December 2021 Sco Cisco Under Vulnerability in BroadWorks Investigation Apache Log4j Cisco Products: December 2021 Sco Cisco Under Vulnerability in December 2021 Sco Products: December 2021	Cisco			Under					
Secure Library Affecting Cisco Products: Cisco Products: Cisco Products: Cisco Application December 2021					on				
Mobility Client December 2021									
Client Cisco Application Policy Infrastruc- ture Controller (APIC) Sco ASR Investigation Apache Log4j Folioy Cisco ASR Apache Log4j Folioy Folioy Folioy Folioy Cisco ASR Apache Log4j Folioy Fo									
isco Cisco Application Investigation Investigation Investigation Investigation Infrastructure Controller (APIC) Social Cisco ASR Under Vulnerability in Apache Log4j (Cisco Products: December 2021 (Controller (APIC) (Cisco Products: December 2021 (Cisco Products: Cisco P									
plication Investigation Apache Log4j Library Affecting	isco			Under					
Policy Infrastruc- ture Controller (APIC) isco Cisco ASR Duder Vulnerability in Apache Log4j Broadcloud Calling Cisco Cisco Products: December 2021 Library Affecting Cisco Products: December 2021 Cisco Produ	ше	-			on				
Infrastruc- ture December 2021 Controller (APIC) isco Cisco ASR Under Vulnerability in 5000 Series Investigation Apache Log4j Routers Library Affecting Cisco Products: December 2021 isco Cisco Under Vulnerability in Broadcloud Investigation Apache Log4j Calling Library Affecting Cisco Products: December 2021 isco Cisco Under Vulnerability in Broadcloud Investigation Apache Log4j Cisco Products: December 2021 isco Products: December 2021 isco Products: December 2021 isco Products: December 2021 isco Cisco Under Vulnerability in BroadWorks Investigation Apache Log4j Library Affecting Cisco Products: December 2021 isco Cisco Under Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021 isco Products: December 2021 isco Products: December 2021 isco Products: December 2021 isco Products: December 2021 Vulnerability in Apache Log4j S800 Series Under Vulnerability in Apache Log4j S800 Series Library Affecting Vineless Cisco Products:		-		investigat.					
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$									
Controller (APIC) isco Cisco ASR Under Vulnerability in 5000 Series Investigation Apache Log4j Routers Library Affecting Cisco Products: December 2021 isco Cisco Under Vulnerability in Broadcloud Investigation Apache Log4j Calling Library Affecting Cisco Products: December 2021 isco Cisco Under Vulnerability in Library Affecting Cisco Products: December 2021 isco Cisco Under Vulnerability in BroadWorks Investigation Apache Log4j Library Affecting Cisco Products: December 2021 isco Cisco Under Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021 isco Cisco Under Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021 isco Products: December 2021 isco Library Affecting Cisco Products: December 2021 isco Cisco Under Vulnerability in Library Affecting Cisco Products: December 2021 isco Cisco Library Affecting Cisco Products: December 2021 Isco Cisco Library Affecting Cisco Products: December 2021 Isco Cisco Library Affecting Cisco Products:									
(APIC) Cisco ASR Under Under Vulnerability in Apache Log4j Routers Library Affecting Cisco Products: December 2021 Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021 Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021 Library Affecting Cisco Products: December 2021 Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021 Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021 Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021 Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021 Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021 Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021 Vulnerability in Catalyst Julnerability in Apache Log4j Library Affecting Cisco Products: December 2021 Vulnerability in Apache Log4j Library Affecting Cisco Products: Cisco Products:						December 2021			
Sisco Cisco ASR Under Vulnerability in 5000 Series Investigation Apache Log4j Routers Library Affecting Cisco Products: December 2021 Sisco Cisco Under Vulnerability in Apache Log4j Calling Library Affecting Cisco Products: December 2021 Cisco Products: December 2021 Calling Library Affecting Cisco Products: December 2021 Cisco Products:									
Foundary Series Foundary Affecting Cisco Products: December 2021 Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021 Sisco Products: Foundary Series Foundary Series Foundary Series Foundary Series Foundary Series Foundary Series Foundary Apache Log4j Foundary Series Foundary Series Foundary Series Foundary Affecting Foundary Series Foundary Affecting Foundary Series Foundary Series Foundary Foundary Foundary Series Foundary Series Foundary Foundary Foundary Series Foundary Series Foundary Foundary Foundary Foundary Foundary Foundary Foundary Foundary Foundary Foundary Foundary Foundary Foundary Foundary Foundary Foundary Foundary Foundary Foundary Foundary Foundary Foundary Foundary F	isco			Under		Vulnerability in			
Routers Routers Library Affecting Cisco Products: December 2021 Sco Cisco Under Vulnerability in Broadcloud Investigation Calling Cisco Products: December 2021 Calling Cisco Products: December 2021 Sco Cisco Under Vulnerability in BroadWorks Investigation Apache Log4j Library Affecting Cisco Products: December 2021 Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021 Sco Cisco Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021 Sco Cisco Vinlerability in Apache Log4j Library Affecting Cisco Products: December 2021 Vulnerability in Catalyst Javanta Apache Log4j Sco Virless Virless Cisco Products:	500				on				
Cisco Products: December 2021 Co Cisco Under Vulnerability in Broadcloud Investigation Apache Log4j Calling Cisco Products: December 2021 Co Cisco Under Vulnerability in BroadWorks Investigation Apache Log4j Library Affecting Cisco Products: December 2021 Cisco Products: De				IIIvestigat.	on				
December 2021 Sco Cisco Under Vulnerability in Broadcloud Investigation Apache Log4j Calling Cisco Products: December 2021 Sco Cisco Under Vulnerability in BroadWorks Investigation Apache Log4j Library Affecting Cisco Products: December 2021 Apache Log4j Library Affecting Cisco Products: December 2021 Sco Cisco Products: December 2021 Sco Cisco Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021 Sco Cisco Under Vulnerability in Apache Log4j Apache		Houters							
SCO Cisco Under Vulnerability in Broadcloud Investigation Apache Log4j Calling Cisco Products: December 2021 SCO Cisco Under Vulnerability in BroadWorks Investigation Apache Log4j Library Affecting Cisco Products: December 2021 SCO Cisco Under Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021 SCO Cisco Under Vulnerability in Catalyst Investigation Apache Log4j 9800 Series Library Affecting Cisco Products:									
Broadcloud Calling Calling Cisco Products: December 2021 Sco Cisco BroadWorks Investigation Apache Log4j Cisco Products: December 2021 Cisco Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021 Cisco Products:	500	Cigao		Undon					
Calling Cisco Products: December 2021 SCO Cisco Under Vulnerability in BroadWorks Investigation Apache Log4j Library Affecting Cisco Products: December 2021 SCO Cisco Products: December 2021 SCO Cisco Vulnerability in Catalyst Investigation Apache Log4j Vulnerability in Catalyst Investigation Apache Log4j SCO Vulnerability in Catalyst Under Cisco Vulnerability in Catalyst Under Cisco	SCO				an a				
Cisco Products: December 2021 isco Cisco Under Vulnerability in BroadWorks Investigation Apache Log4j Library Affecting Cisco Products: December 2021 isco Cisco Under Vulnerability in Catalyst Investigation Apache Log4j 9800 Series Wireless Library Affecting Cisco Products:				mvestigat.	OII	2 0			
December 2021 Sico Cisco Under Vulnerability in BroadWorks Investigation Apache Log4j Library Affecting Cisco Products: December 2021 Sico Cisco Under Vulnerability in Catalyst Investigation Apache Log4j 9800 Series Wireless Library Affecting Cisco Products: Cisco Products: Cisco Products: Cisco Products: Cisco Products: Cisco Products:		Calling							
isco Cisco Under Vulnerability in BroadWorks Investigation Apache Log4j Library Affecting Cisco Products: December 2021 isco Cisco Under Vulnerability in Catalyst Investigation Apache Log4j 9800 Series Wireless Library Affecting Cisco Products: Cisco Products: Cisco Products: Cisco Products: Cisco Products: Cisco Products:									
BroadWorks Investigation Apache Log4j Library Affecting Cisco Products: December 2021 isco Cisco Under Vulnerability in Catalyst Investigation Apache Log4j 9800 Series Wireless Library Affecting Cisco Products:		C:		TT., J.,,					
Library Affecting Cisco Products: December 2021 Sisco Cisco Under Vulnerability in Catalyst Investigation Apache Log4j 9800 Series Wireless Cisco Products: Cisco Products: December 2021 Vulnerability in Apache Log4j Cisco Products:	isco		_						
Cisco Products: December 2021 isco Cisco Under Vulnerability in Catalyst Investigation Apache Log4j 9800 Series Wireless Cisco Products:		Droad Works	•	mvestigat	OII				
December 2021 Vulnerability in Catalyst Investigation Apache Log4j 9800 Series Wireless Cisco Products:									
isco Cisco Under Vulnerability in Catalyst Investigation Apache Log4j 9800 Series Library Affecting Wireless Cisco Products:									
Catalyst Investigation Apache Log4j 9800 Series Library Affecting Wireless Cisco Products:	!:aaa	Ciana		II. J					
9800 Series Library Affecting Wireless Cisco Products:	ISCO								
Wireless Cisco Products:				Investigat	on				
Controllers December 2021									
		Controllers				December 2021			

Vendor	Product Ver	sion(s) Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cisco	Cisco	Affected	No	Vulnerability in			
	CloudCen-			Apache Log4j			
	ter Suite			Library Affecting			
	Admin			Cisco Products:			
				December 2021			
Cisco	Cisco	Under		Vulnerability in			
	CloudCen-	Investigat	ion	Apache Log4j			
	ter			Library Affecting			
	Workload			Cisco Products:			
	Manager			December 2021			
Cisco	Cisco	Under		Vulnerability in			
	Cognitive	Investigat	ion	Apache Log4j			
	Intelligence			Library Affecting			
				Cisco Products:			
				December 2021			
Cisco	Cisco	Affected	No	Vulnerability in			
	Computer			Apache Log4j			
	Telephony			Library Affecting			
	Integration			Cisco Products:			
	Object			December 2021			
	Server						
	(CTIOS)						
Cisco	Cisco	Under		Vulnerability in			
	Connected	Investigat	ion	Apache Log4j			
	Grid			Library Affecting			
	Device			Cisco Products:			
	Manager			December 2021			
Cisco	Cisco	Under		Vulnerability in			
	Connected	Investigat	ion	Apache Log4j			
	Mobile			Library Affecting			
	Experiences			Cisco Products:			
				December 2021			
Cisco	Cisco	Under		Vulnerability in			
	Connectivity	Investigat	ion	Apache Log4j			
				Library Affecting			
				Cisco Products:			
				December 2021			
Cisco	Cisco	Under		Vulnerability in			
	Contact	Investigat	ion	Apache Log4j			
	Center			Library Affecting			
	Domain			Cisco Products:			
	Manager			December 2021			
	(CCDM)						

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cisco	Cisco		Under		Vulnerability in			
	Contact		Investigati	on	Apache Log4j			
	Center				Library Affecting			
	Manage-				Cisco Products:			
	ment				December 2021			
	Portal							
	(CCMP)							
Cisco	Cisco		Affected	No	Vulnerability in			
	Crosswork				Apache Log4j			
	Change				Library Affecting			
	Automation				Cisco Products:			
					December 2021			
Cisco	Cisco CX		Under		Vulnerability in			
	Cloud		Investigati	on	Apache Log4j			
	Agent				Library Affecting			
	Software				Cisco Products:			
					December 2021			
Cisco	Cisco Data		Under		Vulnerability in			
	Center		Investigati	on	Apache Log4j			
	Network		0		Library Affecting			
	Manager				Cisco Products:			
	(DCNM)				December 2021			
Cisco	Cisco		Under		Vulnerability in			
	Defense		Investigati	on	Apache Log4j			
	Orchestrator				Library Affecting			
					Cisco Products:			
					December 2021			
Cisco	Cisco DNA		Under		Vulnerability in			
	Assurance		Investigati	on	Apache Log4j			
					Library Affecting			
					Cisco Products:			
					December 2021			
Cisco	Cisco DNA		Under		Vulnerability in			
	Center		Investigati	on	Apache Log4j			
					Library Affecting			
					Cisco Products:			
					December 2021			
Cisco	Cisco DNA		Under		Vulnerability in			
	Spaces		Investigati	on	Apache Log4j			
	-		Ŭ		Library Affecting			
					Cisco Products:			
					December 2021			

Vendor	Product	Version(s)	Status Update	e Available	Vendor Link	Notes	Other References	Last Updated
Cisco	DUO		Under					
	network		Investigation					
	gateway							
	(on-							
	prem/self-							
a.	hosted)		TT 1		77.1 1.11.			
Cisco	Cisco		Under		Vulnerability in			
	Elastic Services		Investigation		Apache Log4j			
	Controller				Library Affecting Cisco Products:			
	(ESC)				December 2021			
Cisco	Cisco		Under		Vulnerability in			
21500	Emergency		Investigation		Apache Log4j			
	Responder		mvestigation		Library Affecting			
	Troop officer				Cisco Products:			
					December 2021			
Cisco	Cisco		Under		Vulnerability in			
	Enterprise		Investigation		Apache Log4j			
	Chat and				Library Affecting			
	Email				Cisco Products:			
					December 2021			
Cisco	Cisco		Under		Vulnerability in			
	Enterprise		Investigation		Apache Log4j			
	NFV				Library Affecting			
	Infrastruc-				Cisco Products:			
	ture				December 2021			
	Software							
Cisco	(NFVIS) Cisco		Affected No		Vulnerability in			
CISCO	Evolved		Affected No		Apache Log4j			
	Pro-				Library Affecting			
	grammable				Cisco Products:			
	Network				December 2021			
	Manager							
Cisco	Cisco		Under		Vulnerability in			
	Extensible		Investigation		Apache Log4j			
	Network		_		Library Affecting			
	Controller				Cisco Products:			
	(XNC)				December 2021			
Cisco	Cisco		Under		Vulnerability in			
	Finesse		Investigation		Apache Log4j			
					Library Affecting			
					Cisco Products:			
					December 2021			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cisco	Cisco		Under		Vulnerability in			
	Firepower		Investigat	ion	Apache Log4j			
	Manage-				Library Affecting			
	ment				Cisco Products:			
	Center				December 2021			
Cisco	Cisco		Under		Vulnerability in			
	Firepower		Investigat	ion	Apache Log4j			
	Threat		0		Library Affecting			
	Defense				Cisco Products:			
	(FTD)				December 2021			
isco	Cisco		Under		Vulnerability in			
12000	GGSN		Investigat	ion	Apache Log4j			
	Gateway		111,0501800	1011	Library Affecting			
	GPRS				Cisco Products:			
	Support				December 2021			
	Node				Becciniser 2021			
isco	Cisco		Under		Vulnerability in			
isco	HyperFlex		Investigat	ion	Apache Log4j			
	System		mvestigat	1011	Library Affecting			
	Dystem				Cisco Products:			
					December 2021			
sco	Cisco		Under		Vulnerability in			
SCO	Identity		Investigat	ion	Apache Log4j			
	Services		Hivestigat	ion	Library Affecting			
					Cisco Products:			
	Engine				December 2021			
co	(ISE) Cisco		Affected	No				
CO			Affected	NO	Vulnerability in			
	Integrated				Apache Log4j			
	Manage-				Library Affecting Cisco Products:			
	ment				December 2021			
	Controller				December 2021			
	(IMC)							
	Supervisor		II J		17-1			
sco	Cisco		Under	:	Vulnerability in			
	Intersight		Investigat	1011	Apache Log4j			
					Library Affecting			
					Cisco Products:			
·	C:		A.C 1	M -	December 2021			
Cisco	Cisco		Affected	No	Vulnerability in			
	Intersight				Apache Log4j			
	Virtual				Library Affecting			
	Appliance				Cisco Products:			
					December 2021			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cisco	Cisco IOS and IOS XE Software		Under Investigati	on	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco IoT Field Network Director (formerly Cisco Connected Grid Network Manage- ment System)		Under Investigati	on	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco IoT Operations Dashboard		Under Investigati	on	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco IOx Fog Director		Under Investigati	on	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco IP Services Gateway (IPSG)		Under Investigati	on	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Kinetic for Cities		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco MDS 9000 Series Multilayer Switches		Under Investigati	on	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Meeting Server		Under Investigati	on	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 MME Mobility		Under Investigation	on	Vulnerability in Apache Log4j Library Affecting		_	
	Manage- ment Entity				Cisco Products: December 2021			
Cisco	Cisco		Under		Vulnerability in			
	Modeling Labs		Investigation	on	Apache Log4j Library Affecting Cisco Products:			
C:	C:		TT 1		December 2021			
Cisco	Cisco Network		Under		Vulnerability in			
	Assessment		Investigation	OH .	Apache Log4j Library Affecting			
	(CNA)				Cisco Products:			
	Tool				December 2021			
Cisco	Cisco		Under		Vulnerability in			
	Network		Investigation	on	Apache Log4j			
	Assurance		0		Library Affecting			
	Engine				Cisco Products:			
					December 2021			
Cisco	Cisco		Under		Vulnerability in			
	Network		Investigation	on	Apache Log4j			
	Conver-				Library Affecting			
	gence				Cisco Products: December 2021			
	System 2000 Series				December 2021			
Cisco	Cisco		Under		Vulnerability in			
	Network		Investigation	on	Apache Log4j			
	Planner		O		Library Affecting			
					Cisco Products:			
					December 2021			
Cisco	Cisco		Under		Vulnerability in			
	Nexus 5500		Investigation	on	Apache Log4j			
	Platform				Library Affecting			
	Switches				Cisco Products:			
Cisco	Cisco		Under		December 2021 Vulnerability in			
JISCO	Nexus 5600		Investigation	on.	Apache Log4j			
	Platform		Investigatio	511	Library Affecting			
	Switches				Cisco Products:			
					December 2021			
Cisco	Cisco		Under		Vulnerability in			
	Nexus 6000		Investigation	on	Apache Log4j			
	Series		Ü		Library Affecting			
	Switches				Cisco Products:			
					December 2021			

Vendor	Product	Version(s)	Status	Update	e Available	Vendor Link	Notes	Other References	Last Updated
Cisco	Cisco		Under			Vulnerability in			
	Nexus 7000		Investigat	ion		Apache Log4j			
	Series		O .			Library Affecting			
	Switches					Cisco Products:			
						December 2021			
Cisco	Cisco		Under			Vulnerability in			
1000	Nexus 9000		Investigat	ion		Apache Log4j			
	Series		11110501541	1011		Library Affecting			
	Fabric					Cisco Products:			
	Switches in					December 2021			
	Applica-					December 2021			
	tion								
	Centric								
	Infrastruc-								
	ture (ACI)								
	mode		TT 1			37.1 1.11.			
isco	Cisco		Under			Vulnerability in			
	Nexus		Investigat	ion		Apache Log4j			
	Dashboard					Library Affecting			
	(formerly					Cisco Products:			
	Cisco Ap-					December 2021			
	plication								
	Services								
	Engine)								
co	Cisco		Under			Vulnerability in			
	Nexus		Investigat	ion		Apache Log4j			
	Data					Library Affecting			
	Broker					Cisco Products:			
						December 2021			
sco	Cisco		Under			Vulnerability in			
	Nexus		Investigat	ion		Apache Log4j			
	Insights					Library Affecting			
						Cisco Products:			
						December 2021			
sco	Cisco		Under			Vulnerability in			
	Optical		Investigat	ion		Apache Log4j			
	Network		O .			Library Affecting			
	Planner					Cisco Products:			
	-					December 2021			
lisco	Cisco		Affected	No		Vulnerability in			
	Packaged					Apache Log4j			
	Contact					Library Affecting			
	Center					Cisco Products:			
	Enterprise					December 2021			
	Puror brise					December 2021			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cisco	Cisco		Under		Vulnerability in			
	Paging		Investigati	on	Apache Log4j			
	Server				Library Affecting			
	(InformaCas	t)			Cisco Products:			
					December 2021			
Cisco	Cisco		Under		Vulnerability in			
	Paging		Investigati	on	Apache Log4j			
	Server				Library Affecting			
					Cisco Products:			
					December 2021			
Cisco	Cisco		Under		Vulnerability in			
	PDSN/HA		Investigati	on	Apache Log4j			
	Packet				Library Affecting			
	Data				Cis co Products:			
	Serving				December 2021			
	Node and							
	Home							
	Agent							
Cisco	Cisco PGW		Under		Vulnerability in			
	Packet		Investigati	on	Apache Log4j			
	Data				Library Affecting			
	Network				Cisco Products:			
	Gateway				December 2021			
Cisco	Cisco		Under		Vulnerability in			
	Policy		Investigati	on	Apache Log4j			
	Suite				Library Affecting			
					Cisco Products:			
					December 2021			
Cisco	Cisco		Under		Vulnerability in			
	Prime		Investigati	on	Apache Log4j			
	Central for				Library Affecting			
	Service				Cisco Products:			
	Providers				December 2021			
Cisco	Cisco		Under		Vulnerability in			
	Prime Col-		Investigati	on	Apache Log4j			
	laboration				Library Affecting			
	Manager				Cisco Products:			
					December 2021			
Cisco	Cisco		Under		Vulnerability in			
	Prime Col-		Investigati	on	Apache Log4j			
	laboration				Library Affecting			
	Provisioning				Cisco Products:			
					December 2021			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cisco	Cisco		Under		Vulnerability in			
	Prime		Investigation	on	Apache Log4j			
	Infrastructur	e			Library Affecting			
					Cisco Products:			
					December 2021			
Cisco	Cisco		Under		Vulnerability in			
	Prime		Investigation	on	Apache Log4j			
	License				Library Affecting			
	Manager				Cisco Products:			
					December 2021			
Cisco	Cisco		Under		Vulnerability in			
	Prime		Investigation	on	Apache Log4j			
	Network				Library Affecting			
					Cisco Products:			
					December 2021			
Cisco	Cisco		Under		Vulnerability in			
	Prime		Investigation	on	Apache Log4j			
	Optical for				Library Affecting			
	Service				Cisco Products:			
	Providers				December 2021			
Cisco	Cisco		Under		Vulnerability in			
	Prime		Investigation	on	Apache Log4j			
	Provisioning				Library Affecting			
					Cisco Products:			
					December 2021			
Cisco	Cisco		Under		Vulnerability in			
	Prime		Investigation	on	Apache Log4j			
	Service		0		Library Affecting			
	Catalog				Cisco Products:			
					December 2021			
Cisco	Cisco		Under		Vulnerability in			
	Registered		Investigation	on	Apache Log4j			
	Envelope				Library Affecting			
	Service				Cisco Products:			
					December 2021			
Cisco	Cisco		Under		Vulnerability in			
	SD-WAN		Investigation	on	Apache Log4j			
	vEdge 1000		O		Library Affecting			
	Series				Cisco Products:			
	Routers				December 2021			
Cisco	Cisco		Under		Vulnerability in			
	SD-WAN		Investigation	on	Apache Log4j			
	vEdge 2000		G		Library Affecting			
	Series				Cisco Products:			
	Routers				December 2021			

/endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cisco	Cisco		Under		Vulnerability in			
	SD-WAN		Investigat	ion	Apache Log4j			
	vEdge 5000		0		Library Affecting			
	Series				Cisco Products:			
	Routers				December 2021			
Cisco	Cisco		Under		Vulnerability in			
	SD-WAN		Investigat	ion	Apache Log4j			
	vEdge		O		Library Affecting			
	Cloud				Cisco Products:			
	Router				December 2021			
	Platform							
Cisco	Cisco		Under		Vulnerability in			
	SD-WAN		Investigat	ion	Apache Log4j			
	vManage		111,000,1900	1011	Library Affecting			
	vivianage				Cisco Products:			
					December 2021			
lisco	Cisco		Under		Vulnerability in			
1500	Secure		Investigat	ion	Apache Log4j			
	Network		mvestigat	ion	Library Affecting			
	Analytics				Cisco Products:			
	(SNA),				December 2021			
	formerly				December 2021			
	Stealthwatch	h						
sco	Cisco	ш	Under		Vulnerability in			
SCO	SocialMiner		Investigat	ion	Apache Log4j			
	Socialivilliei		Hivestigat	ion	Library Affecting			
					Cisco Products:			
					December 2021			
SCO	Cisco		Under		Vulnerability in			
3CO	TelePres-			:				
			Investigat	1011	Apache Log4j			
	ence				Library Affecting Cisco Products:			
	Manage-							
	ment				December 2021			
	Suite		A.C 1	3.7	37.1 1.11.			
isco	Cisco UCS		Affected	No	Vulnerability in			
	Director				Apache Log4j			
					Library Affecting			
					Cisco Products:			
	aa-				December 2021			
Cisco	Cisco UCS		Under		Vulnerability in			
	Perfor-		Investigat	ion	Apache Log4j			
	mance				Library Affecting			
	Manager				Cisco Products:			
					December 2021			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cisco	Cisco Umbrella		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Unified Attendant Console Advanced		Under Investigati	on	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Unified Attendant Console Business Edition		Under Investigati	on	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Unified Attendant Console Department Edition		Under Investigati	on	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Unified Attendant Console Enterprise Edition		Under Investigati	on	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Unified Attendant Console Premium Edition		Under Investigati	on	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			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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 Investigati	on	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Unified Intelligent Contact Manage- ment 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 Surveil- lance 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 Investigati	on	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Virtualized Voice Browser		Under Investigati	on	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Vision Dynamic Signage Director		Under Investigati	on	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 WAN Automa- tion Engine (WAE)		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Web Security Appliance (WSA)		Under Investigation	on	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Webex Cloud- Connected UC (CCUC)		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Webex Meetings Server		Affected	No	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Webex Teams		Under Investigation	on	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			
Cisco	Cisco Wide Area Appli- cation Services (WAAS)		Under Investigation	on	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	on				
Cisco	Exony Virtualized Interaction Manager (VIM)		Under Investigation	on	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	Managed Services Accelerator (MSX) Network Access Control Service		Under Investigati	on	Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021			

Crix Citrix All Platforms Not Ci ADC Affected (NetScaler ADC) and Citrix Gateway (NetScaler Gateway)	c u in g a a to in o C m c c so v I in ti	Citrix continues to nvestigate any potential mpact on Citrix-managed cloud services. If, as the investigation continuous to the continuous continuous continuous to the continuous continuous to the continuous to	12/21/2021
ADC Affected (NetScaler ADC) and Citrix Gateway (NetScaler	c u in g a a to in o C m c c so v I in ti	contin- ues to nvesti- gate any po- cential ampact on Citrix- managed cloud ser- vices. If, as the investi- gation	
(NetScaler ADC) and Citrix Gateway (NetScaler	in g a to in o o o o o o o o o o o o o o o o o o	envesti- gate any po- cential ampact on Citrix- managed cloud ser- vices. If, as the envesti- gation	
ADC) and Citrix Gateway (NetScaler	in g a to in o o o o o o o o o o o o o o o o o o	envesti- gate any po- cential ampact on Citrix- managed cloud ser- vices. If, as the envesti- gation	
Citrix Gateway (NetScaler	a to to in o o o o o o o o o o o o o o o o o o	any po- cential mpact on Citrix- managed cloud ser- vices. If, as the investi- gation	
Gateway (NetScaler	a to to in o o o o o o o o o o o o o o o o o o	any po- cential mpact on Citrix- managed cloud ser- vices. If, as the investi- gation	
(NetScaler	to in or	mpact on Citrix- managed cloud ser- vices. If, as the investi- gation	
	in o C m c c se v Ii ti	impact on Citrix- managed cloud ser- vices. If, as the investi- gation	
	o C n c se v I i t i i g c c c	citrix- managed cloud ser- vices. If, as the investi- gation	
	or o	Citrix- managed cloud ser- vices. If, as the investi- gation	
	n c ss v Ii t in g	managed cloud ser-vices. If, as che envestigation	
	c se v Ii ti ii g	cloud ser- vices. If, as the nvesti- gation	
	v Ii ti ii g	ser- vices. If, as the nvesti- gation	
	v Ii ti ii g	vices. If, as the investi- gation	
	If ti in g c	If, as the investi- gation	
	ti ii g c	the nvesti- gation	
	in g c	nvesti- gation	
	g c	gation	
	c		
		:OHUIII-	
	u		
		ies,	
	a	any	
		Citrix-	
		managed	
		services	
		are	
		found	
		to be	
		af-	
		fected	
		by this	
		ssue,	
		Citrix	
	W	will	
	t	take	
	iı	mme-	
	d	diate	
		action	
		to	
		remedi-	
		ate the	
		prob-	
		em.	
		Cus-	
		tomers	
		using	
	u C	Citrix-	
		managed	
		cloud	
		services	
71		do not	
		need to	
		take	
	a	any	
	a	action.	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Citrix	Citrix Ap-	All Platforms	Not		Citrix Statement	Citrix		12/21/2021
	plication		Affected			contin-		, ,
	Delivery					ues to		
	Manage-					investi-		
	ment					gate		
	(NetScaler					any po-		
	MAS)					tential		
	,					impact		
						on		
						Citrix-		
						managed		
						cloud		
						ser-		
						vices.		
						If, as		
						the		
						investi-		
						gation		
						contin-		
						ues,		
						any Citrix-		
						managed		
						services		
						are		
						found		
						to be		
						af-		
						fected		
						by this		
						issue,		
						Citrix		
						will		
						take		
						imme-		
						diate		
						action		
						to		
						remedi-		
						ate the		
						prob-		
						lem.		
						Cus-		
						tomers		
						using		
						Citrix-		
						managed		
						cloud		
						services		
					70	do not		
					72	need to		
						take		
						any		
						action.		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
litrix	Citrix		Not		Citrix Statement	Citrix		12/21/2021
	Cloud		Affected			contin-		
	Connector					ues to		
						investi-		
						gate		
						any po-		
						tential		
						impact		
						on		
						Citrix-		
						managed		
						cloud		
						ser-		
						vices.		
						If, as		
						the		
						investi-		
						gation		
						contin-		
						ues,		
						any		
						Citrix-		
						managed .		
						services		
						are		
						found		
						to be		
						af-		
						fected		
						by this		
						issue,		
						Citrix		
						will		
						take		
						imme-		
						diate		
						action		
						to remedi-		
						ate the		
						prob-		
						lem.		
						Cus-		
						tomers		
						using		
						Citrix-		
						managed		
						cloud		
						services		
						do not		
					73	need to		
						take		
						vane		
						any		

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
ndor	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 Citrixmanaged 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		Last Updated 12/21/2021
					74	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		Not		Citrix Statement	Citrix		12/21/2021
	Content		Affected			contin-		
	Collabora-					ues to		
	tion					investi-		
	(ShareFile					gate		
	Integra-					any po-		
	tion) $-$					tential		
	Citrix Files					impact		
	for					on		
	Windows,					Citrix-		
	Citrix Files					managed		
	for Mac,					cloud		
	Citrix Files					ser-		
	for Outlook					vices.		
						If, as		
						the		
						investi-		
						gation		
						contin-		
						ues,		
						any		
						Citrix-		
						managed services		
						are found		
						to be		
						af-		
						fected		
						by this		
						issue,		
						Citrix		
						will		
						take		
						imme-		
						diate		
						action		
						to		
						remedi-		
						ate the		
						prob-		
						lem.		
						Cus-		
						tomers		
						using		
						Citrix-		
						managed		
						cloud		
						services		
					75	do not		
					75	need to		
						take		
						any		
						CULLY		

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
itrix	Citrix		Affected	Yes	Citrix Statement	For	12/21/2021
	Endpoint					CVE-	
	Manage-					2021-	
	ment					44228	
	(Citrix					and	
	XenMobile					CVE-	
	Server)					2021-	
						45046:	
						Impacted-	
						Customers	
						are	
						advised	
						to	
						apply	
						the	
						latest	
						CEM	
						rolling	
						patch	
						up-	
						dates	
						listed	
						below	
						as soon	
						as pos-	
						sible to	
						reduce	
						the risk	
						of ex-	
						ploita-	
						tion.	
						XenMo-	
						bile	
						Server	
						10.14	
						RP2;	
						XenMo-	
						bile	
						Server	
						10.13	
						RP5;	
						and	
						XenMo-	
						bile	
						Server	
						10.12 BB10	
						RP10.	
						Note:	
						Cus-	
					76	tomers	
						who	
						have	
						up-	
						graded	
						their	
						XenMo-	
						bile	
						Server	
						to the	
						11D-	

up-

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
ndor	Citrix Hypervisor (XenServer)	Version(s)	Status Not Affected	Update Available	Vendor Link Citrix Statement	Citrix continues to investigate any potential impact on Citrixmanaged 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		Last Updated 12/21/2021
					77	using Citrix- managed cloud services do not need to take any action.		

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
endor	Product Citrix License Server	Version(s)	Status Not Affected	Update Available	Vendor Link Citrix Statement	Citrix continues to investigate any potential impact on Citrixmanaged 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. Cus-		Last Updated 12/21/2021
					78	tomers using Citrix- managed cloud services do not need to take any action.		

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
litrix	Citrix	All Platforms	Not		Citrix Statement	Citrix		12/21/2021
	SD-WAN		Affected			contin-		
						ues to		
						investi-		
						gate		
						any po-		
						tential		
						impact		
						on		
						Citrix-		
						managed		
						cloud		
						ser-		
						vices.		
						If, as		
						the		
						investi-		
						gation		
						contin-		
						ues,		
						any		
						Citrix-		
						managed		
						services		
						are		
						found		
						to be		
						af-		
						fected		
						by this		
						issue,		
						Citrix		
						will		
						take		
						imme-		
						diate		
						action		
						to		
						remedi-		
						ate the		
						prob-		
						lem.		
						Cus-		
						tomers		
						using		
						Citrix-		
						managed		
						cloud		
						services		
					79	do not		
						need to		
						take		
						any		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Citrix	ShareFile		Not		Citrix Statement	Citrix		12/21/2021
	Storage		Affected			contin-		
	Zones					ues to		
	Controller					investi-		
						gate		
						any po-		
						tential		
						impact		
						on		
						Citrix-		
						managed		
						cloud		
						ser-		
						vices.		
						If, as		
						the investi-		
						gation		
						contin-		
						ues, any		
						Citrix-		
						managed		
						services		
						are		
						found		
						to be		
						af-		
						fected		
						by this		
						issue,		
						Citrix		
						will		
						take		
						imme-		
						diate		
						action		
						to		
						remedi-		
						ate the		
						prob-		
						lem.		
						Cus-		
						tomers		
						using		
						Citrix-		
						managed		
						cloud		
						services		
					80	do not		
						need to		
						take		
						any		
						action.		

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
itrix	Citrix Virtual		Affected		Citrix Statement	IMPAC'	TED:	12/21/2021
	Apps and					VDA		
	Desktops					(non-		
	(XenApp &					LTSR		
	XenDesktop)					ver-		
	1,					sions		
						only)-		
						CVE-		
						2021-		
						44228		
						and		
						CVE-		
						2021-		
						45046:		
						Cus-		
						tomers		
					are			
					advised			
						to		
						apply		
						the		
						latest		
						update		
						as soon		
						as pos-		
						sible to		
						reduce		
						the risk		
						of ex-		
						ploita-		
						tion.		
						Linux		
						Virtual		
						Deliv-		
						ery		
						Agent		
						2112.		
						See the		
						Citrix		
						State-		
						ment		
						for ad-		
						ditional		
						mitiga-		
						tions.		
						For		
						CVE-		
						2021-		
					81	45105:		
					01	Investi-		
						gation		
						has		
						shown		
						that		
						Linux		
						VDA is		
						not im-		
						pacted.		
						Nonethe		

Nonethe-

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
itrix	Citrix	All Platforms	Not		Citrix Statement	Citrix		12/21/2021
	Workspace		Affected			contin-		
	App					ues to		
						investi-		
						gate		
						any po-		
						tential		
						impact		
						on		
						Citrix-		
						managed		
						cloud		
						ser-		
						vices.		
						If, as		
						the		
						investi-		
						gation		
						contin-		
						ues,		
						any		
						Citrix-		
						managed		
						services		
						are found		
						to be		
						af-		
						fected		
						by this		
						issue,		
						Citrix		
						will		
						take		
						imme-		
						diate		
						action		
						to		
						remedi-		
						ate the		
						prob-		
						lem.		
						Cus-		
						tomers		
						using		
						Citrix-		
						managed		
						cloud		
						services		
					82	do not		
					52	need to		
						take		
						any		
						action.		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Claris					Claris Article			
Cloudera	AM2CM		Not		https://my.			
	Tool		Affected		cloudera.com/			
					knowledge/TSB-			
					2021-545-			
					Critical-			
					vulnerability-in-			
					log4j2-CVE-			
					2021-44228?id=			
					332019			
Cloudera	Ambari	Only versions 2.x,	A ffootod		https://my.			
Cioudera	Allibari	1.x	Affected		cloudera.com/			
		1.X						
					knowledge/TSB- 2021-545-			
					Critical-			
					vulnerability-in-			
					log4j2-CVE-			
					2021-44228?id=			
					332019			
Cloudera	Arcadia	Only version	Affected		https://my.			
	Enterprise	se 7.1.x			cloudera.com/			
				knowledge/TSB-				
					2021-545-			
					Critical-			
					vulnerability-in-			
				log4j2-CVE-				
					2021-44228?id =			
					332019			
Cloudera		Only version 6.x	Affected		https://my.			
	and HDF				cloudera.com/			
					knowledge/TSB-			
					2021-545-			
					Critical-			
					vulnerability-in-			
					log4j2-CVE-			
					2021-44228?id =			
					332019			
Cloudera	CDP Oper-		Not		https://my.			
	ational		Affected		cloudera.com/			
	Database				knowledge/TSB-			
	(COD)				2021-545-			
	` /				Critical-			
					vulnerability-in-			
					log4j2-CVE-			
					2021-44228?id=			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cloudera	CDP Private Cloud Base	Only version 7.x	Affected		https://my. cloudera.com/ knowledge/TSB- 2021-545- Critical- vulnerability-in- log4j2-CVE- 2021-44228?id= 332019			
Cloudera	CDS 3 Powered by Apache Spark	All versions	Affected		https://my. cloudera.com/ knowledge/TSB- 2021-545- Critical- vulnerability-in- log4j2-CVE- 2021-44228?id= 332019			
Cloudera	CDS 3.2 for GPUs	All versions	Affected		https://my. cloudera.com/ knowledge/TSB- 2021-545- Critical- vulnerability-in- log4j2-CVE- 2021-44228?id= 332019			
Cloudera	Cloudera Cybersecu- rity Platform	All versions	Affected		https://my. cloudera.com/ knowledge/TSB- 2021-545- Critical- vulnerability-in- log4j2-CVE- 2021-44228?id= 332019			
Cloudera	Cloudera Data Engi- neering (CDE)		Affected		https://my. cloudera.com/ knowledge/TSB- 2021-545- Critical- vulnerability-in- log4j2-CVE- 2021-44228?id= 332019			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cloudera	Cloudera Data Engi- neering (CDE)	All versions	Affected		https://my. cloudera.com/ knowledge/TSB- 2021-545- Critical- vulnerability-in- log4j2-CVE- 2021-44228?id= 332019			
Cloudera	Cloudera Data Flow (CFM)		Affected		https://my. cloudera.com/ knowledge/TSB- 2021-545- Critical- vulnerability-in- log4j2-CVE- 2021-44228?id= 332019			
Cloudera	Cloudera Data Science Workbench (CDSW)	Only versions 2.x, 3.x	Affected		https://my. cloudera.com/ knowledge/TSB- 2021-545- Critical- vulnerability-in- log4j2-CVE- 2021-44228?id= 332019			
Cloudera	Cloudera Data Visu- alization (CDV)		Affected		https://my. cloudera.com/ knowledge/TSB- 2021-545- Critical- vulnerability-in- log4j2-CVE- 2021-44228?id= 332019			
Cloudera	Cloudera Data Warehouse (CDW)		Affected		https://my. cloudera.com/ knowledge/TSB- 2021-545- Critical- vulnerability-in- log4j2-CVE- 2021-44228?id= 332019			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cloudera	Cloudera Data Warehouse (CDW)	All versions	Affected		https://my. cloudera.com/ knowledge/TSB- 2021-545- Critical- vulnerability-in- log4j2-CVE- 2021-44228?id= 332019			
Cloudera	Cloudera DataFlow (CDF)		Affected		https://my. cloudera.com/ knowledge/TSB- 2021-545- Critical- vulnerability-in- log4j2-CVE- 2021-44228?id= 332019			
Cloudera	Cloudera Edge Man- agement (CEM)	All versions	Affected		https://my. cloudera.com/ knowledge/TSB- 2021-545- Critical- vulnerability-in- log4j2-CVE- 2021-44228?id= 332019			
Cloudera	Cloudera Enterprise	Only version 6.x	Affected		https://my. cloudera.com/ knowledge/TSB- 2021-545- Critical- vulnerability-in- log4j2-CVE- 2021-44228?id= 332019			
Cloudera	Cloudera Flow Man- agement (CFM)	All versions	Affected		https://my. cloudera.com/ knowledge/TSB- 2021-545- Critical- vulnerability-in- log4j2-CVE- 2021-44228?id= 332019			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cloudera	Cloudera Machine Learning (CML)		Affected		https://my. cloudera.com/ knowledge/TSB- 2021-545- Critical- vulnerability-in- log4j2-CVE- 2021-44228?id=			
Cloudera	Cloudera Machine Learning (CML)	All versions	Affected		332019 https://my. cloudera.com/ knowledge/TSB- 2021-545- Critical- vulnerability-in-			
Cloudera	Cloudera Manager (Including Backup	All versions	Affected		log4j2-CVE- 2021-44228?id= 332019 https://my. cloudera.com/ knowledge/TSB- 2021-545-			
Cl. 1	Disaster Recovery (BDR) and Replication Manager)		A.C 1		Critical- vulnerability-in- log4j2-CVE- 2021-44228?id= 332019			
Cloudera	Cloudera Manager (Including Backup Disaster Recovery (BDR) and Replication Manager)	Only versions 7.0.x, 7.1.x, 7.2.x	Affected		https://my. cloudera.com/ knowledge/TSB- 2021-545- Critical- vulnerability-in- log4j2-CVE- 2021-44228?id= 332019			
Cloudera	Cloudera Manager (Including Backup Disaster Recovery (BDR))		Not Affected		https://my. cloudera.com/ knowledge/TSB- 2021-545- Critical- vulnerability-in- log4j2-CVE- 2021-44228?id= 332019			

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Cloudera	Hortonworks DataPlane Platform		Not Affected		https://my. cloudera.com/ knowledge/TSB- 2021-545- Critical- vulnerability-in- log4j2-CVE- 2021-44228?id= 332019			
Cloudera	Management Console	All versions	Affected		https://my. cloudera.com/ knowledge/TSB- 2021-545- Critical- vulnerability-in- log4j2-CVE- 2021-44228?id= 332019			
Cloudera	Management Console for CDP Public Cloud		Not Affected		https://my. cloudera.com/ knowledge/TSB- 2021-545- Critical- vulnerability-in- log4j2-CVE- 2021-44228?id= 332019			
Cloudera	Replication Manager		Affected		https://my. cloudera.com/ knowledge/TSB- 2021-545- Critical- vulnerability-in- log4j2-CVE- 2021-44228?id= 332019			
Cloudera	SmartSense		Under Investigati	on	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 Update
Cloudera	Workload		Not		https://my.			
	Manager		Affected		cloudera.com/			
					knowledge/TSB-			
					2021-545-			
					Critical-			
					vulnerability-in-			
					log4j2-CVE-			
					2021-44228?id=			
					332019			
Cloudera	Workload		Not		https://my.			
	XM (SaaS)		Affected		cloudera.com/			
					knowledge/TSB-			
					2021-545-			
					Critical-			
					vulnerability-in-			
					log4j2-CVE-			
					2021-44228?id=			
					332019			
Cloudera	Workload	All versions	Affected		https://my.			
Cioudera	XM	All versions	Allected		cloudera.com/			
	AM							
					knowledge/TSB-			
					2021-545-			
					Critical-			
					vulnerability-in-			
					log4j2-CVE-			
					2021-44228?id =			
					332019			
CloudFlare	;				CloudFlare Blog			
					Post			
Cloudian					Cloudian Article			
HyperStore	2							
	Ecosystem	All	Affected	Yes	Cloudogu			
21044084	2000,000111		111100000	200	Community			
Cloudogu	SCM-		Not		SCM-Manager			
Cioudogu	Manager		Affected		Blog			
C11	manager		Affected					
Cloudron					Cloudron Forum			
Clover	G 1 12	0.04	F	**	Clover Article			40 100 100 -
Code42	Code42	8.8.1	Fixed	Yes	Code42 Release			12/22/2021
	App				Notification			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Code42	Crashplan	8.8, possibly prior versions	Fixed	Yes	Code42 Release Notification	I think, they don't specify in the notice, but we know that they released an updated Crashplan client. Possibly prior versions		12/16/2021
CodeBeam	ner				CodeBeamer	affected.		
Codesys Cohesity					Link Codesys News Cohesity Support Link			
CommVau	lt				CommVault			
Concourse	Concourse		Not affected		Documentation Concourse Community			
ConcreteC	MS.com				Discussion ConcreteCMS.com			
Confluent	Confluent Cloud	N/A	Fixed		Link December 2021 Log4j Vulnerabilities			12/17/2021
Confluent	Confluent Platform	<7.0.1	Affected	Yes	Advisory December 2021 Log4j Vulnerabilities			12/17/2021
Confluent	Confluent for Kubernetes	N/A	Not Affected		Advisory December 2021 Log4j Vulnerabilities Advisory			12/17/2021

Kaffa	Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Confinent Conf	Confluent	Confluent	N/A	Not	N/A	December 2021			12/17/2021
Confluent Conf		Kafka		Affected		Log4j			
Confluent Conf		Connectors				Vulnerabilities			
Elastic Servi Sink Comeetor Confluent Conflu						Advisory			
Search Sink	Confluent	Confluent	<11.1.7	Affected	Yes	December 2021			12/17/2021
Confident Conf		Elastic-				Log4j			
Confluent		Search Sink				Vulnerabilities			
Confident		Connector				Advisory			
Coogle	Confluent	Confluent	< 1.1.5	Affected	Yes	December 2021			12/17/2021
DataProc Sink		Google				Log4j			
Confluent Conf									
Confluent		Sink				Advisory			
Solunk Sink Vulnerabilities Vulnerabilities Vulnerabilities Vulnerabilities Advisory		Connector							
Sink Commetor Confluent	Confluent	Confluent	< 2.05	Affected	Yes	December 2021			12/17/2021
Confluent		Splunk				Log4j			
Confluent		Sink				Vulnerabilities			
HDFS 2 Sink Vulnerabilities Connector Confluent Conflu		Connector				Advisory			
Sink	Confluent	Confluent	<10.1.3	Affected	Yes	December 2021			12/17/2021
Sink Connect		HDFS 2				Log4j			, ,
Confluent Confluent Confluent HDFS 3		Sink							
HDFS 3		Connector				Advisory			
Sink	Confluent	Confluent	<1.1.8	Affected		December 2021			12/17/2021
Confluent Conf		HDFS 3				Log4j			
Confluent		Sink				Vulnerabilities			
VMWare Log4j Tanzu Vulnerabilities GemFire Advisory Sink Connector Connect2id Connect2id Blog Post ConnectWise ConnectWise ContrastSecurity ContrastSecurity ControlUp ControlUp Link COPADATA Support Services CouchBase CouchBase CPanel CPanel Forms Cradlepoint Cradlepoint Crestron 12/20/2021		Connector				Advisory			
Tanzu GemFire GemFire Sink Connector Connect2id ConnectWise ContrastSecurity ControlUp COPADATA Support Services CouchBase Forums CPanel CPanel CPanel CPanel Cradlepoint Crestron Not Crestron I2/20/2021	Confluent	Confluent	< 1.0.8	Affected	Yes	December 2021			12/17/2021
GemFire Sink Connector Connect2id ConnectWise ConnectWise ContrastSecurity ControlUp Link ControlUp Link CoPADATA Support Services CouchBase Forums CouchBase Forums Cradlepoint Cradlepoint Cradlepoint Crestron Not Crestron I2/20/2021		VMWare							
Sink Connector Connect2id Connect2id Blog Post ConnectWise ConnectWise ContrastSecurity ContrastSecurity ContrastSecurity ControlUp ControlUp COPADATA COPADATA Support Services CouchBase CouchBase CouchBase ControlUp CouchBase CouchBas						Vulnerabilities			
Connect2id Connect2id Blog Post ConnectWise ConnectWise Advisory Link ContrastSecurity ControlUp Link COPADATA COPADATA CouchBase CouchBase Forums CPanel CPanel CPanel Crestron Not Corestron ControlUp ControlUp Crestron 12/20/2021						Advisory			
Connect2id Connect2id Blog Post ConnectWise ConnectWise ConnectWise Advisory Link ContrastSecurity ContrastSecurity Article ControlUp ControlUp Link COPADATA COPADATA Support Services CouchBase Forums CPanel Cradlepoint Crestron Not Crestron 12/20/2021									
ConnectWise ConnectWise ConnectWise Advisory Link ContrastSecurity ContrastSecurity Article ControlUp ControlUp ControlUp Link COPADATA COPADATA Support Services CouchBase Forums CPanel Cradlepoint Crestron Not Crestron ConnectWise Advisory Link ContrastSecurity Article ControlUp Link ControlUp Link CopADATA Support Services CouchBase Forums Crestron Crestron Crestron Crestron ConnectWise Advisory Link ContrastSecurity Article ControlUp Link CopADATA Support Services CouchBase									
ConnectWise ContrastSecurity ContrastSecurity ContrastSecurity ControlUp ControlUp ControlUp Link COPADATA COPADATA Support Services CouchBase Forums CPanel Cradlepoint Crestron Not ControlUp ControlUp Link COPADATA Support Services CouchBase Forums CPanel Cradlepoint Crestron Not Crestron I2/20/2021	Connect2id	l							
Advisory Link ContrastSecurity ControlUp ControlUp ControlUp Link COPADATA COPADATA CouchBase Co									
ContrastSecurity Article ControlUp COPADATA COPADATA COUCHBase CouchBase CouchBase CouchBase CouchBase CouchBase CouchBase CouchBase Forums CPanel Cradlepoint Crestron Not Crestron ControlUp Link COPADATA Support Services CouchBase Forums Crestron Crestron CouchBase Forums Crestron Crestron CouchBase Forums Crestron CouchBase Forums Crestron Crestron Crestron Crestron Crestron CouchBase Forums Crestron Crestron Crestron Crestron Crestron CouchBase Forums Crestron Crestron Crestron Crestron Crestron Crestron Crestron Crestron CouchBase Forums Crestron Crest	ConnectW	ise							
Article ControlUp COPADATA COPADATA COPADATA Support Services CouchBase Forums CPanel Cradlepoint Crestron Not ControlUp Link ControlUp Link ControlUp Link ControlUp Link Copanel Copanel Copanel Copanel Crestron Copanel Crestron Crestron Copanel Copanel Copanel Crestron Copanel Crestron Copanel Crestron Copanel Crestron Copanel Copanel Copanel Crestron Copanel Cop									
ControlUp COPADATA COPADATA COPADATA Support Services CouchBase CouchBase Forums CPanel Cradlepoint Crestron Not ControlUp Link COPADATA Support Services CouchBase Forums Cradlepoint Crestron ControlUp Link Copadata Copadata Copadata Support Services CouchBase Forums CouchBase Forums Crestron Crestron Crestron Crestron Copadata Copada	ContrastSe	ecurity							
COPADATA COPADATA Support Services CouchBase CouchBase Forums CPanel Cradlepoint Crestron Not COPADATA Support Services CouchBase Forums Cradlepoint Crestron Crestron COPADATA Support Services CouchBase Forums CouchBase Forums Crestron Crestron Support Services CouchBase Forums Crestron Support Services CouchBase Forums Crestron Crestron Support Services Crestron Support Services CouchBase Forums Crestron Support Services Forums Crestron Support Services CouchBase Forums Crestron Support Services Forums Forum									
Support Services CouchBase CouchBase Forums CPanel Cradlepoint Crestron Not Crestron Support Services CouchBase Forums CouchBase Forums Cradlepoint Crestron Support Services CouchBase Forums Cradlepoint Crestron Support Services CouchBase Forums Crestron Forums Crestron Support Services CouchBase Forums Crestron Forums Crestron Support Services CouchBase Forums Crestron Support Services Forums Forums Crestron Support Services Forums Forums Crestron Support Services Forums Foru									
CouchBase CouchBase Forums CPanel CPanel Cradlepoint Crestron Not Crestron CouchBase Forums CPanel Forms Cradlepoint Crestron Crestron Crestron CouchBase Forums CPanel Forms Crestron Crestron Crestron Crestron Crestron CouchBase Forums Crestron CPanel Forms Crestron Crestr	COPADAT	l'A							
Forums CPanel CPanel Forms Cradlepoint Crestron Not Crestron Forums Crestron Forums CPanel Forms Cradlepoint Crestron 12/20/2021	a								
CPanel Cradlepoint Cradlepoint Crastron Not Crestron Crestron Cradlepoint Crestron C	CouchBase	,							
Cradlepoint Cradlepoint Crestron Not Crestron 12/20/2021	an :								
Crestron Not Crestron $12/20/2021$									
		it		2-					10 10 - 1
Affected Advisory	Crestron								12/20/2021
	CrushFTP			Affected		Advisory			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
CryptShare	e				Cryptshare			
Orrhon A ml-	Duirilanad	N/A	Fixed	Yes	Support Link CyberArk		This advisory is available	19/14/9091
CyberArk	Privileged Threat	N/A	rixea	res	Cyberark Customer Force		This advisory is available to customers only and has	12/14/2021
	Analytics				Customer Force		not been reviewed by	
	(PTA)						CISA.	
Cybereason	` /				Cybereason Blog		CISII.	
V					Post			
CyberRes					CyberRes			
					Community Link			
DarkTrace					DarkTrace			
					Customer Portal			
Dassault					Dassault			
Systèmes					Systemes Link			
Databricks	•				Databricks			
) o to al	Doto 1	× 6 17 0	D: J	Voc	Google Doc			
Datadog	Datadog Agent	>=6.17.0, <=6.32.2,	Fixed	Yes	Datadog Log4j Vulnerability			
	Agent	$\leq = 0.32.2,$ >=7.17.0,			Update			
		>-7.17.0, <=7.32.2			Opaate			
Dataminer		_1.02.2			Dataminer			
3 00 00 11 11 10 1					Community Link			
Oatev					Datev			
					Community Link			
Oatto					Datto Link			
lCache.org	g				dCache.org Link			
Debian					Debian Tracker			
					Link			
Deepinstin	ct				Deepinstinct			
Doll	Alionerana	NT / A	Not	NI / A	Link			19 /15 /9091
Dell	Alienware Command	N/A	Not Affected	N/A	Dell Response to Apache Log4j			12/15/2021
	Center		Allected		Remote Code			
	Control				Execution Execution			
					Vulnerability			
					(CVE-2021-			
					44228)			
Dell	Alienware	N/A	Not	N/A	Dell Response to			12/15/2021
	OC		Affected		Apache Log4j			
	Controls				Remote Code			
					Execution			
					Vulnerability			
					(CVE-2021-			
					44228)			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link Notes Other References	Last Updated
Dell	Alienware On Screen Display	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	12/15/2021
Dell	Alienware Update	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	12/15/2021
Dell	Atmos	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	12/15/2021
Dell	Azure Stack HCI	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	12/15/2021
Dell	CalMAN Powered Calibration Firmware	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	12/15/2021
Dell	CalMAN Ready for Dell	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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-			12/15/2021
Dell	Chassis Manage- ment Controller (CMC)	N/A	Not Affected	N/A	44228) Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-			12/15/2021
Dell	China HDD Deluxe	N/A	Not Affected	N/A	44228) 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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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
Dell	CyberSense for Power- Protect Cyber Recovery	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell BSAFE Crypto-C Micro Edition	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell BSAFE Crypto-J	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	Dell BSAFE Micro Edition Suite	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell Calibration Assistant	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell Cinema Color	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell Cloud Command Repository Manager	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell Cloud Manage- ment 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		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 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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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
Dell	Dell Data Guardian*	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell Data Protection*	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell Data Recovery Environment	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell Data Vault	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link Notes Other Reference	es Last Updated
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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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
Dell	Dell EMC Disk Library for Mainframe	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell EMC GeoDrive	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell EMC Isilon InsightIQ	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell EMC License Manager	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell EMC Networking Onie	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	Dell EMC OpenMan- age 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 OpenMan- age 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 OpenMan- age 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 Manage ment 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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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 Manage- ment 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 PowerPro- tect 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
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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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 Power- Switch Z9264F- ON BMC Dell EMC Power- Switch 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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	Dell EMC Systems Update (DSU)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell EMC Unisphere 360	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell EMC Virtual Storage Integrator	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell EMC VPLEX	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell EMC XtremIO	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell Encryption Enterprise*	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	Dell Encryption Personal*	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell Endpoint Security Suite Enterprise*	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell Hybrid Client	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell ImageAssist	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell Insights Client	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell Linux Assistant	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	Dell Power Manager	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell Power Manager Lite	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell Precision Optimizer	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell Precision Optimizer for Linux	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell Premier Color	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell Recovery (Linux)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	Dell Remediation Platform	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell Remote Execution Engine (DRONE)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell Security Advisory Update - DSA-2021- 088	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell Security Manage- ment Server & Dell Security Manage- ment Server Virtual*	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell Sup- portAssist SOS	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell Thin OS	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	Dell Threat Defense	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell True Color	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell Trusted Device	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dell Update	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Dream Catcher	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	DUP Creation Service	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	DUP Framework (ISG)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Embedded NAS	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Embedded Service Enabler	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Equallogic PS	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Fluid FS	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	iDRAC Service Module (iSM)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	Infinity MLK (firmware)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Integrated Dell Remote Access Controller (iDRAC)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	ISG Accelerators	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	ISG Board & Electrical	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	IsilonSD Manage- ment Server	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	IVE- WinDiag	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	Mainframe Enablers	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	My Dell	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	MyDell Mobile	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	NetWorker Manage- ment 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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	Networking N-Series	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021-			12/15/2021
Dell	Networking OS 10	N/A	Not Affected	N/A	44228) 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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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	OMNIÁ	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	OpenManage Connec- tions - Nagios	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	OpenManage Connec- tions - 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	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Manager 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 Versi	on(s) Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	OpenManage N/A Network Integration	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	PowerConnect N/A N3200	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	PowerConnect N/A PC2800	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	PowerConnect N/A PC8100	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	PowerEdge N/A BIOS	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	PowerEdge N/A Operating Systems	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	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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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
Dell	SmartByte	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	SMI-S	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)		12/15/2021
Dell	Software RAID	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)		12/15/2021
Dell	Solutions Enabler	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)		12/15/2021
Dell	Solutions Enabler vApp	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)		12/15/2021
Dell	Sonic	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)		12/15/2021
Dell	SRS VE	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)		12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	Storage Center OS and additional SC applications unless otherwise noted	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	SupportAssis Client Commercial	t N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	SupportAssis Client Consumer	t N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	UCC Edge	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Unisphere for PowerMax	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Unisphere for PowerMax vApp	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	Unisphere for VMAX	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Unisphere for VNX	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Update Manager Plugin	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	ViPR Controller	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	VNX1	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	VNX2	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	VPLEX VS2/VS6 / VPLEX Witness	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Vsan Ready Nodes	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Warnado MLK (firmware)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Wyse Proprietary OS (ThinOS)	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	Wyse Windows Embedded Suite	N/A	Not Affected	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)			12/15/2021
Dell	APEX Console	N/A	Fixed	N/A	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	Cloud envi- ron- ment patched		12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other R	eferences	Last Updated									
Dell	APEX Data		Affected	No	Dell Response to Apache Log4j	Cloud envi-		12/15/2021									
	Storage				Remote Code	ron-											
	Services				Execution	ment											
					Vulnerability	patch											
					(CVE-2021-	in											
					44228)	progress											
Dell	Cloud IQ		Fixed	N/A	Dell Response to	Cloud		12/15/2021									
					Apache Log4j	envi-											
				Remote Code	ron-												
					Execution	ment											
					Vulnerability	patched											
					(CVE-2021-												
					44228)												
Dell	Connectrix		Affected	No	Dell Response to	Patch		12/15/2021									
	(Cisco				Apache Log4j	ex-											
	MDS				Remote Code	pected											
	DCNM)				Execution	by											
					Vulnerability	12/23/21											
					(CVE-2021-												
\ 11	α	0.1.1	Affected	NT	44228)	D 4 1		10/17/0001									
Dell	Connectrix	ries	Z.1.1 Affected	Affected No	Dell Response to	Patch		12/15/2021									
	B-Series													Apache Log4j	ex-		
	SANnav				Remote Code	pected											
					Execution	by											
					Vulnerability	3/31/2022											
					(CVE-2021- 44228)												
Dell	Data	Versions between	Affected	Yes	Dell Response to	See		12/15/2021									
en	Data Domain OS	7.3.0.5 and	Affected	Tes	Apache Log4j	DSA-		12/19/2021									
	Domain OS	7.7.0.6; Versions			Remote Code	2021-											
		before 7.6.0.30			Execution	274											
		DCIOIC 1.0.0.00			Vulnerability	214											
					(CVE-2021-												
					44228)												
ell	Dell EMC	"18.2 19.1 19.2	Affected	No	Dell Response to	Patch		12/15/2021									
	Avamar	19.3 19.4"	71110000U	110	Apache Log4j	ex-		12/10/2021									
	11/011101	10.0 10.1			Remote Code	pected											
					Execution	by											
				V (0	Vulnerability	$\frac{12}{20}$											
					(CVE-2021-	//											
					44228)												

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	Dell EMC BSN Controller Node		Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	See DSA- 2021- 305		12/15/2021
Dell	Dell EMC Cloud Disaster Recovery	N/A	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	Patch pending		12/15/2021
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 ex- pected by 12/18/21		12/15/2021
Dell	Enterprise Hybrid Cloud		Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	link		12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	Dell EMC Enterprise Storage Analytics for vRealize Operations	"<6.0.0 6.1.0 6.2.x"	Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	See DSA- 2021- 278		12/15/2021

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated	
ell	Dell EMC	N/A	Affected	N/A	Dell Response to	"Dell		12/15/2021	
	Integrated				Apache Log4j	EMC			
	System for				Remote Code	Inte-			
	Azure				Execution	grated			
	Stack HCI				Vulnerability	System			
					(CVE-2021- 44228)	for			
					44228)	Azure Stack			
						HCI is			
						not im-			
						pacted			
						by this			
					advi-				
						sory. If			
						Dell			
						EMC			
						Suppor-			
						tAssist			
						Enter-			
						prise			
					(SAE)				
						or Dell			
						EMC			
						Secure			
						Con-			
						nect			
						Gate-			
						way			
						(SCG) were			
					option-				
						ally			
						in-			
						stalled			
						with			
						Dell			
						EMC			
						Inte-			
						grated			
						System			
						for			
						Azure			
						Stack			
						HCI			
						moni-			
						tor the			
						follow-			
						ing			
						advi- sories.			
					129	Apply			
						workarou	nd		
						guid-	IIU		
						ance			
						ance			
						remedi-			
						ations			
						as they			
						become			
							avail-		

avail-

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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
Dell	Dell EMC NetWorker Virtual Edition	"19.5.x 19.4.x 19.3.x"	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	Patch ex- pected by 12/20/21		12/15/2021
Dell	Dell EMC NetWorker Server	"19.5.x 19.4.x 19.3.x"	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	Patch ex- pected 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'		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"		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 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 PowerPro- tect 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 PowerPro- tect 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 ex- pected by 12/23/21		12/15/2021
Dell	Dell EMC Recover- Point 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 Recover- Point 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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other I	References	Last Updated
Dell	Dell EMC SRM vApp	Versions before 4.6.0.2	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability	Patch ex- pected by 1/25/2022		12/15/2021
Dell	Dell EMC Streaming Data Platform		Affected	No	(CVE-2021- 44228) Dell Response to Apache Log4j Remote Code Execution	Patch ex- pected by		12/15/2021
	1 KWIOTIII				Vulnerability (CVE-2021- 44228)	12/18/21		
Dell	Dell EMC Unity		Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	Patch ex- pected 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
Dell	Dell Open Manage- ment Enterprise - Modular	<1.40.10	Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	See DSA- 2021- 268		12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	DellEMC OpenMan- age Enterprise Services		Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	Patch ex- pected by 12/20/21		12/15/2021
Dell	OpenManage Enterprise	9	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	Patch ex- pected by 12/19/21		12/15/2021
Dell	Dell EMC Ruckus SmartZone 300 Controller		Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	See DSA- 2021- 303		12/15/2021
Dell	Dell EMC Ruckus SmartZone 100 Controller		Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	See DSA- 2021- 303		12/15/2021
Dell	Dell EMC Ruckus Virtual Software		Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	See DSA- 2021- 303		12/15/2021
Dell	Secure Connect Gateway (SCG) Appliance	"5.00.00 5.00.05 and 4.0.06 and earlier versions (OVF and VHD)"	Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	See DSA- 2021- 282		12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Dell	Secure Connect Gateway (SCG) Policy Manager	"5.00.00.10 5.00.05.10"	Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	See DSA- 2021- 281	12/15/2021
Dell	SRS Policy Manager	7	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	Patch pending	12/15/2021
Dell	Storage Center - Dell Storage Manager		Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	Patch pending	12/15/2021
Dell	SupportAssis Enterprise	st	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	Patch ex- pected by 12/23/21	12/15/2021
Dell	Unisphere Central		Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	Patch ex- pected by 1/10/2022	12/15/2021
Dell	Vblock		Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	Patch pend- ing See vce6771 (re- quires cus- tomer login)	12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dell	VNXe 1600	Versions 3.1.16.10220572 and earlier	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	Patch ex- pected by 12/19/21		12/15/2021
Dell	VNXe 3200	Version 3.1.15.10216415 and earlier	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	Patch ex- pected by 12/19/21		12/15/2021
Dell	VxBlock		Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	"Patch pending See vce6771 (requires customer login)"		12/15/2021
Dell	vRealize Orchestra- tor (vRO) Plug-ins for Dell EMC Storage	Various	Affected		Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	See DSA- 2021- 300		12/15/2021
Dell	vRO Plugin for Dell EMC PowerMax	Version 1.2.3 or earlier	Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	See DSA- 2021- 300		12/15/2021
Dell	vRO Plugin for Dell EMC PowerScale	Version 1.1.0 or earlier	Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	See DSA- 2021- 300		12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
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 ex- pected 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 ex- pected by 12/19/21	12/15/2021
Dell	VMware vRealize Automa- tion 8.x	"8.2 8.3 8.4 8.5 and 8.6"	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	Patch ex- pected by 12/19/21	12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Dell	VMware vRealize Orchestra- tor 8.x	"8.2 8.3 8.4 8.5 and 8.6"	Affected	No	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	Patch ex- pected by 12/19/21	12/15/2021
Dell	Wyse Management Suite	<3.5	Affected	Yes	Dell Response to Apache Log4j Remote Code Execution Vulnerability (CVE-2021- 44228)	See DSA- 2021- 267	12/15/2021
Deltares Denequa Device42	Delft- FEWS	>2018.02	Fixed	No	Deltares Advisory Denequa Link Device42 Link	Mitigations Only	12/22/2021
Diebold	ns All products		Not Affected		https://blog. devolutions.net/ 2021/12/critical- vulnerability-in- log4j/ Diebold Nixdorf		
Nixdorf Digi Internation	CTEK nalG6200 family		Not Affected		Link Digi International Advisory Link		12/21/2021
Digi Internation	CTEK naSkyCloud		Not Affected		Digi International Advisory Link		12/21/2021
Digi Internation	CTEK Z45 nalfamily		Not Affected		Digi International Advisory Link		12/21/2021
Digi Internation	Digi 54xx nafamily		Not Affected		Digi International Advisory Link		12/21/2021
Digi Internation	Digi 63xx nafamily		Not Affected		Digi International Advisory Link		12/21/2021
Digi Internation	Digi Any- nalwhereUSB (G2) family		Not Affected		Digi International Advisory Link		12/21/2021
Digi Internation	Digi Any- nalwhereUSB Plus family		Not Affected		Digi International Advisory Link		12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Digi	Digi		Not		Digi			12/21/2021
nternation	aConnect		Affected		International			, ,
	family				Advisory Link			
igi	Digi		Not		Digi			12/21/2021
	alConnect		Affected		International			, ,
	EZ family				Advisory Link			
Digi	Digi		Not		Digi			12/21/2021
	aConnect IT		Affected		International			/ / -
	family				Advisory Link			
igi	Digi Con-		Not		Digi			12/21/2021
	ahectPort		Affected		International			1-/-1/-0-1
10011100101	family		11110000		Advisory Link			
igi	Digi Con-		Not		Digi			12/21/2021
	ahectPort		Affected		International			12/21/2021
10011140101	LTS family		Timeeted		Advisory Link			
Digi	Digi		Not		Digi			12/21/2021
	alConnect		Affected		International			12/21/2021
10C1 HatiOH	Sensor		Affected		Advisory Link			
	family				Advisory Link			
igi	Digi		Not		Digi			12/21/2021
	alConnect		Affected		International			12/21/2021
пенапоп	WS family		Affected		Advisory Link			
\::			Not		-			19 /91 /9091
igi	Digi				Digi			12/21/2021
nternation	naEmbedded		Affected		International			
	Android		3.T .		Advisory Link			10/01/0001
igi	Digi		Not		Digi			12/21/2021
nternation	aEmbedded		Affected		International			
	Yocto		37 .		Advisory Link			10/01/0001
igi	Digi EX		Not		Digi			12/21/2021
nternation	alrouters		Affected		International			
					Advisory Link			
)igi	Digi IX		Not		Digi			12/21/2021
nternation	alrouters		Affected		International			
					Advisory Link			
)igi	Digi LR54		Not		Digi			12/21/2021
nternation	ıal		Affected		International			
					Advisory Link			
igi	Digi One		Not		Digi			12/21/2021
nternation	alfamily		Affected		International			
					Advisory Link			
igi	Digi		Not		Digi			12/21/2021
nternation	aPassport		Affected		International			•
	family				Advisory Link			
igi	Digi		Not		Digi			12/21/2021
	aPortServer		Affected		International			, ,
	TS family				Advisory Link			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Digi	Digi TX		Not		Digi			12/21/2021
nternation	nalrouters		Affected		International			
					Advisory Link			
Digi	Digi WR11		Not		Digi			12/21/2021
nternation	nal		Affected		International			
					Advisory Link			
)igi	Digi WR21		Not		Digi			12/21/2021
nternation	nal		Affected		International			
					Advisory Link			
)igi	Digi WR31		Not		Digi			12/21/2021
nternation	nal		Affected		International			
					Advisory Link			
)igi	Digi		Not		Digi			12/21/2021
iternation	naWR44R/RR		Affected		International			
					Advisory Link			
igi	Digi WR54		Not		Digi			12/21/2021
nternation	nal		Affected		International			
					Advisory Link			
igi	Digi WR64		Not		Digi			12/21/2021
nternation	nal		Affected		International			
					Advisory Link			
igi	AnywhereUS	SB	Not		Digi			12/21/2021
nternation	naManager		Affected		International			
					Advisory Link			
)igi	Aview		Not		Digi			12/21/2021
nternation	nal		Affected		International			
					Advisory Link			
igi	ARMT		Not		Digi			12/21/2021
iternation	nal		Affected		International			
					Advisory Link			
igi	AVWOB		Not		Digi			12/21/2021
iternation	nal		Affected		International			
					Advisory Link			
igi	Digi		Not		Digi			12/21/2021
nternation	naNavigator		Affected		International			
					Advisory Link			
igi	Digi		Not		Digi			12/21/2021
ternation	$na\mathbb{R}emote$		Affected		International			
	Manager				Advisory Link			
igi	Digi Xbee		Not		Digi			12/21/2021
nternation	nalmobile app		Affected		International			
					Advisory Link			
)igi	Lighthouse		Not		Digi			12/21/2021
nternation	nal		Affected		International			
					Advisory Link			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Digi Internation	Realport al		Not Affected		Digi International Advisory Link			12/21/2021
Digi Internation Digicert	Remote aHub Config Utility		Not Affected		Digi International Advisory Link Digicert Link			12/21/2021
Digital AI DNSFilter					Digital AI Article DNSFilter Blog			
Docker Docusign					Post Docker Blog Post Docusign Alert			
DrayTek	Vigor Routers, Access Points, Switches, VigorACS Central Management Software, MyVigor Platform		Not Affected		DrayTek Statement			12/15/2021
DSpace					DSpace Google Group			
Dynatrace	Managed cluster nodes		Not Affected	No	Official Dynatrace Communication	Please see Dy- natrace Com- munica- tion for details		12/21/2021
Dynatrace	SAAS		Fixed	No	Official Dynatrace Communication			12/21/2021
Dynatrace	FedRamp SAAS		Fixed	No	Official Dynatrace Communication			12/21/2021
Dynatrace	Synthetic public locations		Fixed	No	Official Dynatrace Communication			12/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Dynatrace	Synthetic Private ActiveGate		Fixed	Yes	Official Dynatrace Communication	Please see Dy- natrace Com- munica- tion for details		12/21/2021
Dynatrace	ActiveGate		Not Affected	No	Official Dynatrace Communication			12/21/2021
Dynatrace	OneAgent		Not Affected	No	Official Dynatrace Communication			12/21/2021
Dynatrace	Dynatrace Extensions		Fixed	Yes (See Notes)	Official Dynatrace Communication	Please see Dy- natrace Com- munica- tion for details		12/21/2021
EasyRedm	ine				EasyRedmine News			

/endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Eaton	Undisclosed	Undisclosed	Affected		Security Bulletin	Doesn't	
						openly	
						disclose	
						what	
						prod-	
						ucts	
						are af-	
						fected	
						or not	
						for	
						quote	
						'secu-	
						rity	
						pur-	
						poses'.	
						Needs	
						email	
						regis-	
						tration.	
						No	
						workaround	
						pro-	
						vided	
						due to	
						regis-	
						tration	
						wall.	
clecticIQ					EclecticIQ	waii.	
ciccolora					Advisory		
clipse					Eclipse		
oundation	n				Foundation Wiki		
FI	ш				EFI Link		
Groupwa	ro				EGroupware		
Groupwa	10				Link		
lastic	APM Java		Under		Apache Log4j2		12/15/2021
asuic	Agent		Investigati	on	Remote Code		12/10/2021
	Agent		mvestigati	Oli	Execution (RCE)		
					Vulnerability -		
					CVE-2021-44228		
					- ESA-2021-31		
Clastic	APM		Not				19 /15 /9091
iastic					Apache Log4j2		12/15/2021
	Server		Affected		Remote 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	Beats		Not		Apache Log4j2			12/15/2021
			Affected		Remote Code			
					Execution (RCE)			
					Vulnerability -			
					CVE-2021-44228			
					- ESA-2021-31			
Elastic	Cmd		Not		Apache Log4j2			12/15/2021
			Affected		Remote Code			
					Execution (RCE)			
					Vulnerability -			
					CVE-2021-44228			
					- ESA-2021-31			
Elastic	Elastic		Not		Apache Log4j2			12/15/2021
	Agent		Affected		Remote Code			
					Execution (RCE)			
					Vulnerability -			
					CVE-2021-44228			
					- ESA-2021-31			
Elastic	Elastic		Under		Apache Log4j2			12/15/2021
	Cloud		Investigati	on	Remote Code			
	Enterprise				Execution (RCE)			
					Vulnerability -			
					CVE-2021-44228			
					- ESA-2021-31			
Elastic	Elastic		Under		Apache Log4j2			12/15/2021
	Cloud		Investigati	on	Remote Code			
	Enterprise				Execution (RCE)			
					Vulnerability -			
					CVE-2021-44228			
					- ESA-2021-31			
Elastic	Elastic		Not		Apache Log4j2			12/15/2021
	Cloud on		Affected		Remote Code			
	Kubernetes				Execution (RCE)			
					Vulnerability -			
					CVE-2021-44228			
					- ESA-2021-31			
Elastic	Elastic		Under		Apache Log4j2			12/15/2021
	Cloud		Investigati	on	Remote Code			. ,
			<u> </u>		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 Endgame		Not Affected		Apache Log4j2 Remote Code			12/15/2021
	Ziiagaiiie		Timootou		Execution (RCE)			
					Vulnerability -			
					CVE-2021-44228			
					- ESA-2021-31			
Elastic	Elastic		Not		Apache Log4j2			12/15/2021
	Maps		Affected		Remote Code			7 -7 -
	Service				Execution (RCE)			
					Vulnerability -			
					CVE-2021-44228			
					- ESA-2021-31			
Elastic	Elasticsearch	5,6,8	Affected	Yes	Apache Log4j2			12/15/2021
					Remote Code			, ,
					Execution (RCE)			
					Vulnerability -			
					CVE-2021-44228			
					- ESA-2021-31			
Elastic	Endpoint		Not		Apache Log4j2			12/15/2021
	Security		Affected		Remote Code			
					Execution (RCE)			
					Vulnerability -			
					CVE-2021-44228			
					- ESA-2021-31			
Elastic	Enterprise		Not		Apache Log4j2			12/15/2021
	Search		Affected		Remote Code			
					Execution (RCE)			
					Vulnerability -			
					CVE-2021-44228			
					- ESA-2021-31			
Elastic	Fleet		Not		Apache Log4j2			12/15/2021
	Server		Affected		Remote Code			
					Execution (RCE)			
					Vulnerability -			
					CVE-2021-44228			
					- ESA-2021-31			
Elastic	Kibana		Not		Apache Log4j2			12/15/2021
			Affected		Remote 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	Logstash	<6.8.21,<7.16.1	Affected	Yes	Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31			12/15/2021
Elastic	Machine Learning		Not Affected		Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31			12/15/2021
Elastic	Swiftype		Not Affected		Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31			12/15/2021
ElasticSea			Not					
F11 .	products		Affected	27	T211 - 4			40/45/0004
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 de- ploye- ments expect fixed 12/18/20	021	12/17/2021
Ellucian	Admin		Not Affected		Ellucian Response on Apache Log4j Issue	,,		12/17/2021
Ellucian	Enterprise Identity Services(BE	IS)	Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Banner Integration for eLearning		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Ellucian	Banner Integration for eProcuremen	at .	Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Banner Workflow	11	Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Banner Document Manage- ment (includes Banner Document Retention)		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Ellucian Advance Web Connector		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Ellucian eTranscripts		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Ellucian Mobile		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Ellucian Solution Manager		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Banner Event Publisher		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Banner Self Service		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021
Ellucian	Colleague Analytics		Not Affected		Ellucian Response on Apache Log4j Issue			12/17/2021

Vendor	Product	Version(s) Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Ellucian	CRM	Not		Ellucian			12/17/2021
	Advance	Affected		Response on			
				Apache Log4j			
				Issue			
Ellucian	CRM	Not		Ellucian			12/17/2021
	Advise	Affected		Response on			
				Apache Log4j			
				Issue			
Ellucian	CRM	Not		Ellucian			12/17/2021
	Recruit	Affected		Response on			
				Apache Log4j			
				Issue			
Ellucian	Ellucian	Not		Ellucian			12/17/2021
	Data	Affected		Response on			
	Access			Apache Log4j			
				Issue			
Ellucian	Ellucian	Not		Ellucian			12/17/2021
	Design	Affected		Response on			
	Path			Apache Log4j			
				Issue			
Ellucian	Ellucian	Not		Ellucian			12/17/2021
	ePrint	Affected		Response on			
				Apache Log4j			
				Issue			
Ellucian	Ellucian	Not		Ellucian			12/17/2021
	Ethos API	Affected		Response on			, ,
	& API			Apache Log4j			
	Manage-			Issue			
	ment						
	Center						
Ellucian	Ellucian	Not		Ellucian			12/17/2021
	Ethos	Affected		Response on			, ,
	Extend			Apache Log4j			
				Issue			
Ellucian	Ellucian	Not		Ellucian			12/17/2021
	Ethos	Affected		Response on			, ,
	Integration			Apache Log4j			
	G			Issue			
Ellucian	Ellucian	Not		Ellucian			12/17/2021
	Experience	Affected		Response on			, , , -
				Apache Log4j			
				Issue			
Ellucian	Ellucian	Not		Ellucian			12/17/2021
	Intelligent	Affected		Response on			//
	Platform	111100000		Apache Log4j			
	(ILP)			Issue			
	(1111)			10000			

Vendor	Product Version(s)	Status Update Available	Vendor Link Notes Other References	Last Updated
Ellucian	Ellucian International Student and Scholar Manage- ment (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
Ellucian	Ellucian Messaging Adapter (EMA)	Not Affected	Ellucian Response on Apache Log4j Issue	12/17/2021
Ellucian	Ellucian Payment Gateway	Not Affected	Ellucian Response on Apache Log4j Issue	12/17/2021
Ellucian	Ellucian Ellucian Portal	Not Affected	Ellucian Response on Apache Log4j Issue	12/17/2021
Ellucian	Ellucian Workflow	Not Affected	Ellucian Response on Apache Log4j Issue	12/17/2021
Ellucian	Ellucian PowerCampus	Not Affected	Ellucian Response on Apache Log4j Issue	12/17/2021
Emerson	K-Series Coriolis Transmitters	Not Affected	Emerson Security Notification MR.RMT21003- 2	12/17/2021
Emerson	Prolink Configura- tion 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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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-			12/17/2021
Emerson	5726 Transmitter		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	Plantweb Advisor for Metrology and Metering Suite SDK		Not Affected		Emerson Security Notification MR.RMT21003- 2			12/17/2021
Emerson	Gas Chromatographs: M500/2350A MON2000 700XA/15000 370XA MON2020		Not Affected		Emerson Security Notification MR.RMT21003- 2			12/17/2021
Emerson	Gas Analysis: X- STREAM Enhanced (XEGP XEGK XEGC XEGF XEFD XECLD)		Not Affected		Emerson Security Notification MR.RMT21003- 2			12/17/2021
Emerson	Gas Detection: Millennium II Basic Single & Dual Channel 928 Wireless Gas Monitor/628 Gas Sensor 935 & 936 Open Path Gas Detector Millennium Air Particle Monitor		Not Affected		Emerson Security Notification MR.RMT21003- 2			12/17/2021
Emerson	Monitor K-Series Coriolis Transmitters		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	Prolink Configura- tion 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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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
Emerson	Gas Chromatographs: M500/2350A MON2000 700XA/1500X 370XA MON2020	ζA	Not Affected		Emerson Security Notification EMR.RMT21003- 2			12/17/2021
Emerson	Gas Analysis: X- STREAM Enhanced (XEGP XEGK XEGC XEGF XEFD XECLD)		Not Affected		Emerson Security Notification EMR.RMT21003- 2			12/17/2021
Emerson	Gas Detection: Millennium II Basic Single & Dual Channel 928 Wireless Gas Monitor/628 Gas Sensor 935 & 936 Open Path Gas Detector Millennium Air Particle Monitor		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Emerson	Incus Ultrasonic gas leak detector		Not Affected		Emerson Security Notification EMR.RMT21003- 2			12/17/2021
Emerson	Flame Detection: 975UF & 975UR Infrared Flame Detectors 975HR Infrared Hydrogen Flame Detector 975MR Multi- Spectrum Infrared Flame Detector		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021
Emerson	Liquid Transmit- ters: 5081 1066 1056 1057 56		Not Affected		Emerson Security Notification EMR.RMT21003- 2			12/17/2021
Emerson	Combustion: OCX OXT 6888 CX1100 6888Xi		Not Affected		Emerson Security Notification EMR.RMT21003- 2			12/17/2021
Emerson	Spectrex family Flame Detectors and Rosemount 975 flame detector		Not Affected		Emerson Security Notification EMR.RMT21003- 2			12/17/2021
Emerson	CT4400 QCL General Purpose Continuous Gas Analyzer		Not Affected		Emerson Security Notification EMR.RMT21003- 2			12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Emerson	CT5400 QCL General Purpose Continuous Gas		Not Affected		Emerson Security Notification EMR.RMT21003- 2			12/17/2021
Emerson	Analyzer CT5100 QCL Field Housing Continuous Gas		Not Affected		Emerson Security Notification EMR.RMT21003- 2			12/17/2021
Emerson	Analyzer CT5800 QCL Flameproof Housing Continuous Gas		Not Affected		Emerson Security Notification EMR.RMT21003- 2			12/17/2021
Emerson	Analyzer CT4215 QCL Packaging Leak Detection		Not Affected		Emerson Security Notification EMR.RMT21003- 2			12/17/2021
Emerson	System 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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Emerson	3051 & 3051S Pressure transmitter families		Not Affected		Emerson Security Notification EMR.RMT21003- 2			12/17/2021
Emerson	2051 Pressure Transmit- ter 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 Transmit- ter 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-			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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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-			12/17/2021
Emerson	248 Temperature Transmitter		Not Affected		Emerson Security Notification EMR.RMT21003-			12/17/2021
Emerson	326T Temperature Transmitter		Not Affected		Emerson Security Notification EMR.RMT21003-			12/17/2021
Emerson	327T Temperature Transmitter		Not Affected		Emerson Security Notification EMR.RMT21003-			12/17/2021
Emerson	648 Temperature Transmitter		Not Affected		Emerson Security Notification EMR.RMT21003-			12/17/2021
Emerson	4088 Upgrade Utility		Not Affected		Emerson Security Notification EMR.RMT21003-			12/17/2021
Emerson	Engineering Assistant 5.x & 6.x		Not Affected		Emerson Security Notification EMR.RMT21003-			12/17/2021
Emerson	248 Configuration Application		Not Affected		Emerson Security Notification EMR.RMT21003-			12/17/2021
Emerson	Rosemount IO-Link Assistant		Not Affected		Emerson Security Notification EMR.RMT21003-			12/17/2021
Emerson	Rosemount TankMas- ter and TankMas- ter Mobile		Not Affected		Emerson Security Notification EMR.RMT21003-2			12/17/2021

Vendor	Product	Version(s) Status	Update Available	Vendor Link	Notes Other Refer	ences Last Updated
Emerson	Rosemount RadarMas- ter and RadarMas- ter Plus	Not Affecte	d	Emerson Security Notification EMR.RMT21003- 2		12/17/2021
Emerson	Rosemount Radar Con- figuration Tool	Not Affecte	d	Emerson Security Notification EMR.RMT21003- 2		12/17/2021
Emerson	Rosemount 2460 System Hub	Not Affecte	d	Emerson Security Notification EMR.RMT21003- 2		12/17/2021
Emerson	Rosemount 2410 Tank Hub	Not Affecte	d	Emerson Security Notification EMR.RMT21003- 2		12/17/2021
Emerson	Rosemount 3490 Controller	Not Affecte	d	Emerson Security Notification EMR.RMT21003- 2		12/17/2021
Emerson	Rosemount 2230 Graphical Field Display	Not Affecte	d	Emerson Security Notification EMR.RMT21003- 2		12/17/2021
Emerson	Rosemount 2240S Multi- input Tempera- ture Transmitter	Not Affecte	d	Emerson Security Notification EMR.RMT21003- 2		12/17/2021
Emerson	Rosemount CMS/SCU 51/SCC	Not Affecte	l	Emerson Security Notification EMR.RMT21003- 2		12/17/2021
Emerson	Rosemount CMS/WSU 51/SWF 51	Not Affecte	d	Emerson Security Notification EMR.RMT21003- 2		12/17/2021
Emerson	Rosemount CMS/IOU 61	Not Affecte	d	Emerson Security Notification EMR.RMT21003- 2		12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Emerson	Rosemount Level Transmit- ters (14xx 33xx 53xx 54xx 56xx)		Not Affected		Emerson Security Notification EMR.RMT21003- 2			12/17/2021
Emerson	Rosemount Radar Level Gauges (Pro 39xx 59xx)		Not Affected		Emerson Security Notification EMR.RMT21003- 2			12/17/2021
Emerson	Rosemount Tank Radar Gauges (TGUxx)		Not Affected		Emerson Security Notification EMR.RMT21003- 2			12/17/2021
Emerson	Rosemount Level Detectors (21xx)		Not Affected		Emerson Security Notification EMR.RMT21003- 2			12/17/2021
Emerson	Emerson Aperio software		Not Affected		Emerson Security Notification EMR.RMT21003-			12/17/2021
Enterprise ESET	DT				EnterpriseDT Statement ESET Statement			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
ESRI	ArcGIS Data Store	All	Fixed	Yes	https://www. esri.com/arcgis- blog/products/ arcgis-enterprise/ administration/ arcgis-software- and-cve-2021- 44228-aka- log4shell-aka- logjam/	Requires script remediation. ESRI has created scripts to remove the JndiLook class, but has not issued patches to upgrade the Log4j versions	up	12/17/2021
ESRI	ArcGIS Enterprise	All	Fixed	Yes	https://www. esri.com/arcgis- blog/products/ arcgis-enterprise/ administration/ arcgis-software- and-cve-2021- 44228-aka- log4shell-aka- logjam/	Requires script remediation. ESRI has created scripts to remove the JndiLook class, but has not issued patches to upgrade the Log4j versions	cup	12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
ESRI	ArcGIS GeoEvent Server	All	Fixed	Yes	https://www. esri.com/arcgis- blog/products/ arcgis-enterprise/ administration/ arcgis-software- and-cve-2021- 44228-aka- log4shell-aka- logjam/	Requires script remediation. ESRI has created scripts to remove the JndiLooku class, but has not issued patches to upgrade the Log4j versions	шр	12/17/2021
ESRI	ArcGIS Server	All	Fixed	Yes	https://www. esri.com/arcgis- blog/products/ arcgis-enterprise/ administration/ arcgis-software- and-cve-2021- 44228-aka- log4shell-aka- logjam/	Requires script remediation. ESRI has created scripts to remove the JndiLooku class, but has not issued patches to upgrade the Log4j versions	шр	12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Othe	er References	Last Updated
ESRI	ArcGIS Workflow Manager Server	All	Fixed	Yes	https://www. esri.com/arcgis- blog/products/ arcgis-enterprise/ administration/ arcgis-software- and-cve-2021- 44228-aka- log4shell-aka- logjam/	Requires script remedi- ation. ESRI has created scripts to remove the JndiLookup class, but has not issued patches to up- grade the Log4j		12/17/2021
ESRI	Portal for ArcGIS	All	Fixed	Yes	https://www.esri.com/arcgis-blog/products/arcgis-enterprise/administration/arcgis-software-and-cve-2021-44228-aka-log4shell-aka-logjam/	versions Requires script remedi- ation. ESRI has created scripts to remove the JndiLookup class, but has not issued patches to up- grade the Log4j versions		12/17/2021
Estos					Estos Support Statement			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Evolveum Midpoint Ewon Exabeam					Evolveum Midpoint Statement Ewon Statement Exabeam Statement	This advisory is available to customers only and has not been reviewed by		
Exact Exivity					Exact Statement Exivity Statement	CISA		
ExtraHop	Reveal(x)	<=8.4.6, <=8.5.3, <=8.6.4	Affected	Yes	ExtraHop Statement	Versions >8.4.7, >8.5.4, >8.6.5 and >=8.7 are fixed.		12/21/2021
eXtreme Hosting Extreme Networks					eXtreme Hosting Statement Extreme Networks Statement Extron Statement			
F-Secure	Elements Connector		Affected	Yes	The Log4J Vulnerability (CVE-2021- 44228) – which F-Secure products are affected, what it means, what steps should you take - F-Secure Community			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
F-Secure	Endpoint Proxy	13-15	Affected	Yes	F-Secure services Status - 0-day exploit found in the Java logging package log4j2			
F-Secure	Messaging Security Gateway		Affected	Yes	The Log4J Vulnerability (CVE-2021- 44228) — which F-Secure products are affected, what it means, what steps should you take - F-Secure Community			
F-Secure	Policy Manager	13-15	Affected	Yes	F-Secure services Status - 0-day exploit found in the Java logging package log4j2			
F-Secure	Policy Manager Proxy	13-15	Affected	Yes	F-Secure services Status - 0-day exploit found in the Java logging package log4j2			
F5	BIG-IP (all modules)	11.x - 16.x	Not Affected		F5 Security Advisory			
F5	BIG-IQ Centralized Management	7.x-8.x	Not Affected		F5 Security Advisory			
F5	F5OS	1.x	Not Affected		F5 Security Advisory			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
F5	Traffix SDC	5.x (5.2.0 CF1, 5.1.0 CF-30 - 5.1.0 CF-33)	Affected	No	F5 Security Advisory	Vulnerab compo- nents: EMS- ELK compo- nents (Flu- entd + Elastic Search + Kibana), Ele- ment Man- age- ment		
F5	NGINX Plus	R19 - R25	Not Affected		F5 Security Advisory (CVE- 2021-44228), F5 Security Advisory (CVE-	System		
F5	NGINX Open Source	1.x	Not Affected		2021-45046) F5 Security Advisory (CVE- 2021-44228), F5 Security Advisory (CVE-			
F5	NGINX Unit	1.x	Not Affected		2021-45046) F5 Security Advisory (CVE- 2021-44228), F5 Security Advisory (CVE- 2021-45046)			
F5	NGINX App Protect	3.x	Not Affected		2021-43046) F5 Security Advisory (CVE- 2021-44228), F5 Security Advisory (CVE- 2021-45046)			

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

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
edEx	Ship	Unknown	Affected/	Under	FedEx Statement	Note:		12/15/2021
	Manager		Investigat	ion		FedEx		
	Software					is		
						aware		
						of the		
						issue		
						related		
						to the		
						Log4j		
						Re- mote		
						Code		
					Execu-			
						tion		
						vulner-		
						ability		
						affect-		
						ing		
						various		
						Apache		
						prod-		
						ucts.		
						We are		
						actively		
						assess-		
						ing the		
						situa-		
						tion		
						and		
						taking		
					neces-			
						sary		
						action		
						as		
						appro-		
						priate.		
						As a		
						result,		
						we are		
						tem-		
						porar-		
						ily		
						unable		
						to		
						provide a link		
						to		
						down-		
						load		
						the		
					166	FedEx		
						Ship		
						Man-		
						ager		
						soft-		
						ware or		
						gener-		
						ate		
						prod-		
						prou- nct		

uct

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 FileCataly	rst				FileCapStatement FileCatalyst	required.		
FileCloud					Statement FileCloud			
FileWave					Statement FileWave			
FINVI FireDaemo	on				Statement FINVI Statement FireDemon			
Fisher & Paykel Healthcare Flexagon	<u>a</u>		Not Affected		Statement Fisher & Paykel Healthcare Advisory Link Flexagon Statement			12/21/2021
Flexera					Flexera			
Forcepoint Forcepoint	DLP Manager Forcepoint Cloud Security Gateway (CSG)		Affected Not Affected		Statement Login (forcepoint.com) Login (forcepoint.com)			

Vendor	Product Ve	ersion(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Forcepoint	Next Generation Firewall (NGFW)		Not Affected		Login (forcepoint.com)			
Forcepoint	Next Generation Firewall, NGFW VPN Client, Forcepoint User ID service and Sidewinder		Not Affected		Login (forcepoint.com)			
Forcepoint			Not Affected		Login			
Forcepoint	Endpoint Security Manager (Web, Email and DLP)		Affected		(forcepoint.com) Login (forcepoint.com)			
Forescout	DEI)				Forescout			
ForgeRock	Autonomous Identity		Affected		Statement Security Advisories - Knowledge - BackStage (forgerock.com)	all other Forge- Rock prod- ucts Not vulneral	ble	
Fortinet	FortiAIOps		Affected		PSIRT Advisories FortiGuard	vanicia		
Fortinet	FortiAnalyzer		Not Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiAnalyzer Cloud		Not Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiAP		Not Affected		PSIRT Advisories FortiGuard			
Fortinet	FortiAuthenticat	cor	Not Affected		PSIRT Advisories FortiGuard			

Vendor	Product Version(s)	Status Update Available	Vendor Link	Notes	Other References	Last Updated
Fortinet	FortiCASB	Affected	PSIRT			
			Advisories			
			FortiGuard			
Fortinet	FortiConvertor	Affected	PSIRT			
			Advisories			
			FortiGuard			
Fortinet	FortiDeceptor	Not	PSIRT			
	•	Affected	Advisories			
			FortiGuard			
Fortinet	FortiEDR	Not	PSIRT			
	Agent	Affected	Advisories			
	0		FortiGuard			
Fortinet	FortiEDR	Affected	PSIRT			
	Cloud		Advisories			
			FortiGuard			
Fortinet	FortiGate	Not	PSIRT			
	Cloud	Affected	Advisories			
			FortiGuard			
Fortinet	FortiGSLB	Not	PSIRT			
	Cloud	Affected	Advisories			
	0.10 0.00		FortiGuard			
Fortinet	FortiMail	Not	PSIRT			
		Affected	Advisories			
			FortiGuard			
Fortinet	FortiManager	Not	PSIRT			
1 01 01110 0		Affected	Advisories			
		Timoocou	FortiGuard			
Fortinet	FortiManager	Not	PSIRT			
1 01 01110 0	Cloud	Affected	Advisories			
	01044	Timocod	FortiGuard			
Fortinet	FortiNAC	Affected	PSIRT			
			Advisories			
			FortiGuard			
Fortinet	FortiNAC	Affected	PSIRT			
			Advisories			
			FortiGuard			
Fortinet	FortiOS	Not	PSIRT			
1 01 01110 0	(includes	Affected	Advisories			
	FortiGate	Timoocou	FortiGuard			
	&		2 02 02 04 04 04			
	FortiWiFi)					
Fortinet	FortiPhish	Not	PSIRT			
1 01 011100	Cloud	Affected	Advisories			
	01044	11100004	FortiGuard			
Fortinet	FortiPolicy	Affected	PSIRT			
1 OI UIIICU	1 of the oney	Micolog	Advisories			
			FortiGuard			
			rornGuaru			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Fortinet	FortiPortal		Affected		PSIRT			
					Advisories			
					FortiGuard			
Fortinet	FortiRecord	ler	Not		PSIRT			
			Affected		Advisories			
					FortiGuard			
Fortinet	FortiSIEM		Affected		PSIRT			
					Advisories			
					FortiGuard			
Fortinet	FortiSOAR	,	Affected		PSIRT			
					Advisories			
					FortiGuard			
Fortinet	FortiSwicth	1	Not		PSIRT			
	Cloud in		Affected		Advisories			
	FortiLANC	loud			FortiGuard			
Fortinet	FortiSwitch	1	Not		PSIRT			
	&		Affected		Advisories			
	FortiSwitch	Manager			FortiGuard			
Fortinet	FortiToken		Not		PSIRT			
	Cloud		Affected		Advisories			
					FortiGuard			
Fortinet	FortiVoice		Not		PSIRT			
			Affected		Advisories			
					FortiGuard			
Fortinet	FortiWeb		Not		PSIRT			
	Cloud		Affected		Advisories			
					FortiGuard			
Fortinet	ShieldX		Affected		PSIRT			
					Advisories			
					FortiGuard			
FTAPI					FTAPI			
					Statement			
Fujitsu					Fujitsu			
					Statement			
FusionAut	h FusionAuth	1.32	Not		log4j CVE: How			
			Affected		it affects			
					FusionAuth			
					(TLDR: It			
					doesn't) -			
					FusionAuth			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
GE Digital			Unknown		GE Digital Advisory Link(login required)	This advisory is available to customers only and has not been reviewed by		12/22/2021
GE Digital Grid			Unknown		GE Digital Grid Advisory Link(login required)	CISA. This advi- sory is avail- able to cus- tomers only and has not been re- viewed by CISA.		12/22/2021
GE Gas Power	Baseline Security Center (BSC)		Affected		GE Gas Power Advisory Link	Vulnerab to be fixed by vendor pro- vided workarou No user actions neces- sary. Con- tact GE for details.		12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
GE Gas Power	Baseline Security Center (BSC) 2.0		Affected		GE Gas Power Advisory Link	Vulnerable to be fixed by vendor pro- vided workarou No user actions neces- sary. Con- tact GE for details		12/22/2021
GE Gas Power	Asset Performance Management (APM)		Affected		GE Gas Power Advisory Link	GE verifying workarou	und.	12/22/2021
GE Gas Power	Control Server		Affected		GE Gas Power Advisory Link	The Control Server is Affected via vCenter. There is a fix for vCenter. Please see below. GE verifying the vCenter fix as proposed by the vendor.		12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
GE Gas Power	Tag Mapping Service		Affected	Yes	GE Gas Power Advisory Link	Vulnerabi fixed. No user actions neces- sary. Up- dated to log4j 2.16	lity	12/22/2021
GE Healthcare	9		Unknown		GE Healthcare Advisory Link	This advisory is not available at the time of this review, due to maintence on the GE Healthcare		12/22/2021
Gearset					Gearset Statement	website.		
Genesys GeoServer					Genesys Statement GeoServer			
Gerrit code					Announcement Gerrit Statement			
review GFI Ghidra					GFI Statement Ghidra Statement			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	s Last Updated
Gigamon	Fabric Manager	<5.13.01.02	Affected	Yes	Gigamon Customer Support Portal	Updates avail- able via the Giga- mon Sup- port Portal. This advi- sory avail- able to cus- tomers only and has not been re- viewed by CISA.	12/21/2021
GitHub	GitHub	GitHub.com and GitHub Enterprise Cloud	Fixed		GitHub Statement	CISA.	12/17/2021
GitLab		r			GitLab		
Globus					Statement Globus Statement		
GoAnywhe	ereMFT	< 6.8.6	Affected	Yes	GoAnywhere Statement		12/18/2021
GoAnywhe	ereGateway	< 2.8.4	Affected	Yes	GoAnywhere Statement		12/18/2021
GoAnywhe GoCD	ereMFT Agents	< 1.6.5	Affected	Yes	GoAnywhere Statement GoCD Statement		12/18/2021

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	AI Platform Training and Prediction		Not Affected		https: //cloud.google. com/log4j2- security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Access Transparence	у	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	Actifio		Not		https:	Actifio		12/21/2021
loud			Affected		//cloud.google.	has		
					com/log4j2-	identi-		
					security-advisory	fied limited		
						expo- sure to		
						the		
						Log4j 2		
						vulner-		
						ability		
						and has		
						re-		
						leased		
						a hotfix		
						to		
						address		
						this		
						vulner-		
						ability.		
						Visit		
						https:		
						//now.		
						actifio.		
						com for		
						the full		
						state-		
						ment		
						and to		
						obtain		
						the		
						hotfix		
						(avail- able to		
						Actifio		
						cus-		
						tomers		
						only).		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
oogle	Anthos		Not		https:	Product		12/21/2021
loud			Affected		//cloud.google.	does		
					com/log4j2-	not use		
					security-advisory	Log4j 2		
						and is		
						not im-		
						pacted		
						by the		
						issues		
						identi-		
						fied in CVE-		
						2021-		
						44228		
						and		
						CVE-		
						2021-		
						45046.		
						Cus-		
						tomers		
						may		
						have		
						intro-		
						duced a		
						sepa-		
						rate		
						logging		
						solu-		
						tion		
						that		
						uses		
						Log4j 2.		
						We		
						strongly		
						encour-		
						age		
						cus-		
						tomers		
						who		
						manage		
						Anthos		
						envi-		
						ron-		
						ments		
						to identify		
						compo-		
						nents		
						depen-		
					150	depen-		
					178	Log4j 2		
						and		
						update		
						them		
						to the		
						latest		

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

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

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

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
oogle loud	Anthos on VMWare		Not Affected		https: //cloud.google. com/log4j2- security-advisory	Product does not use Log4j 2 and is not im-	12/21/2021
						pacted by the issues identi-	
						fied in CVE- 2021- 44228	
						and CVE- 2021- 45046. We	
						strongly encour- age	
						cus- tomers to check VMware	
						recom- menda- tions docu-	
						mented in VMSA-	
						2021- 0028 and deploy	
						fixes or workarounds to their VMware	
						prod- ucts as they become	
					182	avail- able. We also recom-	
						mend cus- tomers review	
						their respec- tive applica-	
						tions and	

and

Vendor .	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
endor pogle oud	Product Apigee	Version(s)	Status Not Affected	Update Available	Vendor Link https: //cloud.google. com/log4j2- security-advisory	Notes Apigee installed Log4j 2 in its Apigee Edge VMs, but the software was not used and therefore the VMs were not impacted by the issues in CVE-2021-44228 and CVE-2021-45046. Apigee updated Log4j 2 to v.2.16 as an additional precaution. It is possi-		Last Updated 12/17/2021
					183	ble that cus- tomers may have intro- duced custom		
						re- sources that are using vulner- able ver- sions of Log4i.		

Log4j.

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
endor oogle loud	Product App Engine	Version(s)	Status Not Affected	Update Available	Vendor Link https: //cloud.google. com/log4j2- security-advisory	Notes 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	Other References	Last Updated 12/21/2021
					184	strongly encourage customers who manage App Engine environments to identify components 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	AppSheet		Not		https:	The		12/21/2021
Cloud			Affected		//cloud.google.	App-		
					com/log4j2-	Sheet		
					security-advisory	core plat-		
						form		
						runs on		
						non-		
						JVM		
						(non-		
						Java)		
						based run-		
						times.		
						At this		
						time,		
						we have		
						identi-		
						fied no		
						impact		
						to core App-		
						Sheet		
						func-		
						tional-		
						ity.		
						Addi-		
						tion-		
						ally, we		
						have patched		
						one		
						Java-		
						based		
						auxil-		
						iary		
						service		
						in our		
						plat- form.		
						We will		
						con-		
						tinue to		
						moni-		
						tor for		
						af-		
						fected		
						services and		
					105	patch		
					185	or		
						remedi-		
						ate as		
						re-		
						quired.		
						If you		
						have		
						any		
						ques- tions or		

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

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other Re	eferences	Last Updated
Google Cloud	BigQuery Omni		Not Affected		https://cloud.google.	BigQuery		12/19/2021
Joud	Omni		Апестеа		com/log4j2-	Omni, which		
					security-advisory	runs on		
					security advisory	AWS		
						and		
						Azure		
						infras-		
						truc-		
						ture,		
						does		
						not use		
						Log4j 2		
						and is		
						not im-		
						pacted		
						by the		
						issues		
						identi- fied in		
						CVE-		
						2021-		
						44228		
						and		
						CVE-		
						2021-		
						45046.		
						We con-		
						tinue to		
						work		
						with		
						AWS		
						and		
						Azure		
						to		
						assess		
						the		
						situation.		

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

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

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

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
endor oogle loud	Product Cloud Build	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	Other References	Last Updated 12/21/2021
					195	strongly encourage customers who manage Cloud Build environments to identify components dependent on Log4j 2 and update them to the latest		

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google	Cloud		Not		https:	Product		12/15/2021
Cloud	Composer		Affected		//cloud.google.	does		
					com/log4j2-	not use		
					security-advisory	Log4j 2		
						and is not im-		
						pacted		
						by the		
						issues		
						identi-		
						fied in		
						CVE-		
						2021-		
						44228		
						and		
						CVE-		
						2021-		
						45046.		
						Cloud		
						Com-		
						poser		
						does		
						not use		
						Log4j 2 and is		
						not im-		
						pacted		
						by the		
						issues		
						in		
						CVE-		
						2021-		
						44228		
						and		
						CVE-		
						2021-		
						45046.		
						It is		
						possi-		
						ble that		
						cus-		
						tomers		
						may		
						have im-		
						ported		
						or		
						intro-		
						duced		
					107	other		
					197	depen-		
						dencies		
						via		
						DAGs,		
						in-		
						stalled		
						PyPI		
						mod-		
						ules,		
						plugins,		

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

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

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Google	Cloud		Not		https:	Product	12/21/2021
loud	Functions		Affected		//cloud.google.	does	
					com/log4j2-	not use	
					security-advisory	Log4j 2	
						and is	
						not im-	
						pacted	
						by the	
						issues identi-	
						fied in	
						CVE-	
						2021-	
						44228	
						and	
						CVE-	
						2021-	
						45046.	
						Cus-	
						tomers	
						may	
						have	
						intro-	
						duced a	
						sepa-	
						rate	
						logging	
						solu-	
						tion	
						that	
						uses	
						Log4j 2. We	
						strongly	
						encour-	
						age	
						cus-	
						tomers	
						who	
						manage	
						Cloud	
						Func-	
						tions	
						envi-	
						ron-	
						ments	
						to	
						identify	
						compo-	
					202	nents	
						depen-	
						dent on	
						Log4j 2	
						and	
						update	
						them to the	
						latest	
						version	

version.

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

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

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

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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.		12/21/20	21	

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
loogle	Cloud Run		Not		https:	Product	12/21/2021
loud	for Anthos		Affected		//cloud.google.	does	
					com/log4j2-	not use	
					security-advisory	Log4j 2	
						and is	
						not im-	
						pacted	
						by the issues	
						identi-	
						fied in	
						CVE-	
						2021-	
						44228	
						and	
						CVE-	
						2021-	
						45046.	
						Cus-	
						tomers	
						may	
						have	
						intro-	
						duced a	
						sepa- rate	
						logging	
						solu-	
						tion	
						that	
						uses	
						Log4j 2.	
						We	
						strongly	
						encour-	
						age	
						cus-	
						tomers	
						who	
						manage	
						Cloud Run for	
						Anthos	
						envi-	
						ron-	
						ments	
						to	
						identify	
						compo-	
					209	nents	
					40 <i>3</i>	depen-	
						dent on	
						Log4j 2	
						and	
						update	
						them	
						to the	
						latest	
						vorgion	

version.

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Google	Cloud Shell		Not		https:	Product	12/21/2021
loud			Affected		//cloud.google.	does	
					com/log4j2-	not use	
					security-advisory	Log4j 2	
						and is	
						not im-	
						pacted	
						by the issues	
						identi-	
						fied in	
						CVE-	
						2021-	
						44228	
						and	
						CVE-	
						2021-	
						45046.	
						Cus-	
						tomers	
						may	
						have	
						intro-	
						duced a	
						sepa-	
						rate	
						logging solu-	
						tion	
						that	
						uses	
						Log4j 2.	
						We	
						strongly	
						encour-	
						age	
						cus-	
						tomers	
						who	
						manage	
						Cloud	
						Shell ·	
						envi-	
						ron-	
						ments to	
						identify	
						compo-	
						nents	
					010	depen-	
					212	dent 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	Cloud Source Repositories		Not Affected		https: //cloud.google. com/log4j2- security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/21/2021
Google Cloud	Cloud Spanner		Not Affected		https: //cloud.google. com/log4j2- security-advisory	Product does not use Log4j 2 and is not impacted by the issues identified in CVE-2021-44228 and CVE-2021-45046.		12/19/2021

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

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

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

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

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

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

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

Vendor Pro	roduct Version	(s) Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Dat		Not Affected	Update Available	Vendor Link https: //cloud.google. com/log4j2- security-advisory	Data Cata- log has been up- dated to miti- gate the issues identi- fied in CVE- 2021- 44228 and CVE- 2021- 45046. We strongly encour- age cus- tomers who intro- duced their own connec- tors to	Other References	Last Updated 12/20/2021
					age cus- tomers who intro- duced their own connec-		
					identify depen- dencies on Log4j 2 and update them		
					Log4j 2 and update		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
endor oogle loud	Product Data Fusion	Version(s)	Not Affected Not Affected	Update Available	Vendor Link https: //cloud.google. com/log4j2- security-advisory	Data Fusion does not use Log4j 2, but uses Dat- aproc as one of the options to execute pipelines. Dat- aproc re- leased new images on De- cember 18, 2021 to address the vulner- ability in CVE- 2021- 44228 and CVE-		Last Updated 12/20/2021
					223	2021- 45046. Customers must follow instructions in a notification sent on December 18, 2021 with the subject line "Important information about Data Fusion."		

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

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google	Dataflow		Not		https:	Dataflow		12/17/2021
loud			Affected		//cloud.google.	does		
					com/log4j2- security-advisory	not use		
					security-advisory	Log4j 2 and is		
						not im-		
						pacted		
						by the		
						issues		
						in		
						CVE-		
						2021-		
						44228		
						and		
						CVE-		
						2021-		
						45046.		
						If you		
						have		
						changed		
						depen-		
						dencies		
						or default		
						behav-		
						ior, it is		
						strongly		
						recom-		
						mended		
						you		
						verify		
						there is		
						no		
						depen-		
						dency		
						on vul-		
						nerable		
						ver-		
						sions		
						Log4j 2.		
						Cus-		
						tomers have		
						been		
						pro-		
						vided		
						details		
						and		
						instruc-		
					201	tions in		
					225	a notifi-		
						cation		
						sent on		
						Decem-		
						ber 17,		
						2021		
						with		
						the		
						subject		
						line		

line

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
ndor oogle oud	Product Dataproc Metastore	Version(s)	Status Not Affected	Update Available	Vendor Link https: //cloud.google. com/log4j2- security-advisory	Dataproom 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 instruc-		Last Updated 12/20/2021
					227	infor- mation regard- ing Log4j 2 vulner- ability in your gRPC- enabled Dat-		

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

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

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

Vendor Product Version(s)	Status U _I	pdate Available	Vendor Link	Notes	Other References	Last Updated
Vendor Product Version(s) Google Filestore Cloud	Status U _I Not Affected	odate Available	Vendor Link https: //cloud.google. com/log4j2- security-advisory	Notes Log4j 2 is contained within the File- store service; there is a technical control in place that mitigates the vul- nerabilities in CVE- 2021- 44228 and CVE- 2021- 45046. Log4j 2 will be up- dated to the latest version as part of the sched- uled rollout in Jan-	Other References	Last Updated 12/21/2021

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

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

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

endor	Product	$\operatorname{Version}(s)$	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
oogle	Google		Not		https:	Google		12/21/2021
oud	Kubernetes		Affected		//cloud.google.	Kuber-		
	Engine				com/log4j2-	netes		
					security-advisory	Engine		
						does		
						not use		
						Log4j 2		
						and is not im-		
						pacted		
						by the		
						issues		
						identi-		
						fied in		
						CVE-		
						2021-		
						44228		
						and		
						CVE-		
						2021-		
						45046.		
						Cus-		
						tomers		
						may		
						have		
						intro-		
						duced a		
						sepa- rate		
						logging		
						solu-		
						tion		
						that		
						uses		
						Log4j 2.		
						We		
						strongly		
						encour-		
						age		
						cus-		
						tomers		
						who		
						manage		
						Google		
						Kuber-		
						netes		
						Engine		
						envi- ron-		
						ments		
					235	to		
						identify		
						compo-		
						nents		
						depen-		
						dent on		
						Log4j 2		
						and		
						update		
						them		

them

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

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

ndor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
ogle	Looker		Not		https:	Looker-		12/18/2021
oud			Affected		//cloud.google.	hosted		
					com/log4j2-	in-		
					security-advisory	stances		
						have		
						been		
						up-		
						dated		
						to a		
						Looker		
						version		
						with		
						Log4j		
						v2.16.		
						Looker		
						is cur-		
						rently		
						work-		
						ing		
						with		
						third-		
						party		
						driver		
						vendors		
						to eval-		
						uate		
						the		
						impact		
						of the		
						Log4j vulner-		
						ability. As		
						Looker		
						does		
						not		
						enable		
						logging		
						for		
						these		
						drivers		
						in		
						Looker-		
						hosted		
						in-		
						stances,		
						no mes-		
						sages		
						are		
					000	logged.		
					238	We con-		
						clude		
						that		
						the		
						vulner-		
						ability		
						is miti-		
						gated.		
						We con-		
						tinue to		

tinue to

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

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

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google	Migrate for		Not		https:	M4CE		12/19/2021
Cloud	Compute		Affected		//cloud.google.	has		
	Engine (M4CE)				com/log4j2- security-advisory	been		
	(M4CE)				security-advisory	up- dated		
						to miti-		
						gate		
						the		
						issues		
						identi-		
						fied in		
						CVE- 2021-		
						44228		
						and		
						CVE-		
						2021-		
						45046.		
						M4CE		
						has		
						been		
						up- dated		
						to		
						version		
						4.11.9		
						to		
						address		
						the vul-		
						nerabil- ities. A		
						notifi-		
						cation		
						was		
						sent to		
						cus-		
						tomers		
						on De-		
						cember		
						17, 2021		
						with		
						subject		
						line		
						"Impor-		
						tant		
						infor-		
						mation		
						about CVE-		
					241	2021-		
						44228		
						and		
						CVE-		
						2021-		
						45046"		
						for		
						M4CE		
						V4.11		
						or		

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

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

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

/endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
endor oogle loud	Product Pub/Sub Lite	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 Pub/Sub Lite en-	Last Updated 12/16/2021
					245	viron- ments to identify compo- nents depen- dent on Log4j 2 and update them to the latest	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Google Cloud	reCAPTCE Enterprise	IA	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	Recommend	dations	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	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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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
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

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

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

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

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

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Gradle	Gradle		Not Affected	No	Gradle Blog - Dealing with the critical Log4j vulnerability	Gradle Scala Compiler Plugin de- pends 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 Distri- bution Agent	< 1.6.2	Affected	Yes	Gradle Enterprise Security Advisories - Remote code execution vulnerability due to use of Log4j2			
Grafana					Grafana Statement			
Grandstre	am				Grandstream			
Gravitee	Access Management	3.10.x	Not Affected	No	Statement About the Log4J CVSS 10 Critical Vulnerability			
Gravitee	Access Management	3.5.x	Not Affected	No	About the Log4J CVSS 10 Critical Vulnerability			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Gravitee	API	3.10.x	Not	No	About the Log4J			
	Management		Affected		CVSS 10 Critical			
					Vulnerability			
Gravitee	API	3.5.x	Not	No	About the Log4J			
	Management		Affected		CVSS 10 Critical			
					Vulnerability			
Gravitee	Alert	1.5.x	Not	Yes	About the Log4J			
	Engine		Affected		CVSS 10 Critical			
	_				Vulnerability			
Gravitee	Alert	1.4.x	Not	No	About the Log4J			
	Engine		Affected		CVSS 10 Critical			
	O				Vulnerability			
Gravitee	Cockpit	1.4.x	Not	No	About the Log4J			
	1		Affected		CVSS 10 Critical			
					Vulnerability			
Gravitee.io	1				Gravitee.io			
0101100110					Statement			
Gravwell					Gravwell			
JIWY WCII					Statement			
Graylog	Graylog	All versions >=	Affected	Yes	Graylog Update			
Grayiog	Server	$1.2.0 \text{ and } \leq $	Affected	ies	for Log4j			
	Sel vel	4.2.2			101 L0g4j			
GreenShot		4.2.2			GreenShot			
31 CCHOHOU					Statement			
Guidewire					Guidewire			
Juidewire					Statement			
T A D								
HAProxy					HAProxy			
п Б					Statement			
HarmanPro	0				HarmanPro			
AMX	D 1		3. 7		AMX Statement			
HashiCorp	Boundary		Not		HashiCorp			
			Affected		security bulletin			
					re.			
·• • • · · · ·	~ -				CVE-2021-44228			
HashiCorp	Consul		Not		HashiCorp			
			Affected		security bulletin			
					re.			
					CVE-2021-44228			
HashiCorp			Not		HashiCorp			
	Enterprise		Affected		security bulletin			
					re.			
					CVE-2021-44228			
HashiCorp	Nomad		Not		HashiCorp			
_			Affected		security bulletin			
					re.			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Upda
HashiCorp			Not		HashiCorp			
	Enterprise		Affected		security bulletin			
					re.			
					CVE-2021-44228			
HashiCorp	Packer		Not		HashiCorp			
			Affected		security bulletin			
					re.			
					CVE-2021-44228			
HashiCorp	Terraform		Not		HashiCorp			
1			Affected		security bulletin			
					re.			
					CVE-2021-44228			
HashiCorp	Terraform		Not		HashiCorp			
пастопр	Enterprise		Affected		security bulletin			
	Effect prise		Tinected		re.			
					CVE-2021-44228			
HashiCorp	Vagrant		Not		HashiCorp			
HasinCorp	vagrani		Affected		security bulletin			
			Affected		*			
					re. CVE-2021-44228			
IIl.: C	3714		Not					
HashiCorp	vaun		Affected		HashiCorp			
			Affected		security bulletin			
					re. CVE-2021-44228			
IIl-: C	3714		Not					
HashiCorp					HashiCorp			
	Enterprise		Affected		security bulletin			
					re.			
TT 1.0	***		37.		CVE-2021-44228			
HashiCorp	Waypoint		Not		HashiCorp			
			Affected		security bulletin			
					re.			
	D. T.				CVE-2021-44228			40//-
HCL	BigFix	2.0.1 - 2.0.4	Fixed		KB with fix	Not Af-	Forum post with more	12/15/202
Software	Compliance					fected	specifics	
						for		
						related		
						CVE-		
						2021-		
						45046		
HCL	BigFix	All	Not		KB	Not Af-		12/15/202
Software	Insights		Affected			fected		
						for		
						related		
						CVE-		
						2021-		
						45046		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other Refere	ences Last Updated
HCL Software	BigFix Insights for Vulnerabil- ity Remediation	All	Not Affected		KB	Not Affected for related CVE- 2021- 45046	12/15/2021
HCL Software	BigFix Inventory	< 10.0.7	Fixed		KB with fix	Not Affected for related CVE-2021-45046	12/15/2021
HCL Software	BigFix Lifecycle	All	Not Affected		KB	Not Affected for related CVE-2021-45046	12/15/2021
HCL Software	BigFix Mobile	All	Not Affected		KB	Not Affected for related CVE-2021-45046	12/15/2021
HCL Software	BigFix Patch	All	Not Affected		KB	Not Affected for related CVE-2021-45046	12/15/2021
HelpSyster Clearswift HENIX		1.21.7 - 1.22.9, 2.0.3 - 2.1.5,	Fixed		HelpSystems Clearswift Vendor Link	25020	12/23/2021
Hexagon Hikvision Hitachi Energy Hitachi Vantara	eSOMS	2.2.0 - 3.0.2	Not Affected		Hexagon Statement Hikvision Hitachi Energy Hitachi Vantara		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Update
Honeywell					Honeywell			
					Statement			
HP	Teradici	< v113	Fixed	Yes	Apache Log4j			2021-12-17
	Cloud				update for			
	Access				Teradici PCoIP			
	Controller				Connection			
					Manager,			
					Teradici Cloud			
					Access			
					Connector,			
					Teradici PCoIP			
					License Server,			
					Teradici			
					Management			
					Console, and			
					Teradici EMSDK			
HP	Teradici	< 1.0.6	Fixed	Yes	Apache Log4j			2021-12-17
	EMSDK				update for			
					Teradici PCoIP			
					Connection			
					Manager,			
					Teradici Cloud			
					Access			
					Connector,			
					Teradici PCoIP			
					License Server,			
					Teradici			
					Management			
					Console, and			
					Teradici EMSDK			
HP	Teradici	< 21.10.3	Fixed	Yes	Apache Log4j			2021-12-17
	Manage-				update for			
	ment				Teradici PCoIP			
	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
НР	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			2021-12-17
НР	Teradici PCoIP License Server		Not Affected		Teradici EMSDK Apache Log4j update for Teradici PCoIP Connection Manager, Teradici Cloud Access Connector, Teradici PCoIP License Server, Teradici Management Console, and Teradici EMSDK			2021-12-17
НРЕ	3PAR StoreServ Arrays		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
НРЕ	AirWave Manage- ment Platform		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	Alletra 6000		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
НРЕ	Alletra 9k		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	Aruba Central		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	Aruba ClearPass Policy Manager		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	Aruba ClearPass Policy Manager		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	Aruba Instant (IAP)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	Aruba Location Services		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	Aruba NetEdit		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	Aruba PVOS Switches		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	Aruba SDN VAN Controller	ī	Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	Aruba User Experience Insight (UXI)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	Aruba VIA Client		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	ArubaOS-CX switches		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	ArubaOS-S switches		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
НРЕ	ArubaOS SD-WAN Controllers and Gateways		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	ArubaOS Wi-Fi Controllers and Gateways		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
НРЕ	BladeSystem Onboard Administrato		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
НРЕ	Brocade 16Gb Fibre Channel SAN Switch for HPE Synergy		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	Brocade 16Gb SAN Switch for HPE BladeSys- tem c-Class		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	Brocade 32Gb Fibre Channel SAN Switch for HPE Synergy		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	Brocade		Not		(Revision)	Support		2021-12-12
	Network		Affected		Apache Software	Com-		
	Advisor				Log4j - Security	munica-		
					Vulnerability CVE-2021-44228	tion Cross		
					C V E-2021-44228	Refer-		
						ence ID:		
						SIK7387		
HPE	CloudAuth		Not		(Revision)	Support		2021-12-12
			Affected		Apache Software	Com-		
					Log4j - Security	munica-		
					Vulnerability	tion		
					CVE-2021-44228	Cross		
						Refer-		
						ence ID: SIK7387		
HPE	CloudPhysics		Not		(Revision)	Support		2021-12-12
111 12	Cloudi flysics	•	Affected		Apache Software	Com-		2021-12-12
			Miccoca		Log4j - Security	munica-		
					Vulnerability	tion		
					CVE-2021-44228	Cross		
						Refer-		
						ence ID:		
						SIK7387		
HPE	Compute		Not		(Revision)	Support		2021-12-12
	Cloud		Affected		Apache Software	Com-		
	Console				Log4j - Security	munica-		
					Vulnerability CVE-2021-44228	tion		
					CVE-2021-44228	Cross Refer-		
						ence ID:		
						SIK7387		
HPE	Compute		Not		(Revision)	Support		2021-12-12
	operations		Affected		Apache Software	Com-		-0-1 1- 1-
	manager-				Log4j - Security	munica-		
	$_{ m FW}$				Vulnerability	tion		
	UPDATE				CVE-2021-44228	Cross		
	SERVICE					Refer-		
						ence ID:		
						SIK7387		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
НРЕ	COS (Cray Operating System)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	Cray Systems Manage- ment (CSM)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
НРЕ	Custom SPP Portal Link		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	Data Services Cloud Console		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	Harmony Data Platform		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
НРЕ	HOP public services (grafana, vault, rancher, Jenkins)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence 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 Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
НРЕ	HPE B-series SN4000B SAN Extension Switch		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence 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 Com- munica- tion Cross Refer- ence 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 Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12

HPE		Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
111 12	HPE B-series SN6600B		Not Affected		(Revision) Apache Software Log4j - Security	Support Com- munica-		2021-12-12
	Fibre				Vulnerability	tion		
	Channel				CVE-2021-44228	Cross		
	Switch					Refer-		
						ence ID:		
						SIK7387		
HPE	HPE		Not		(Revision)	Support		2021-12-12
	B-series		Affected		Apache Software	Com-		
	SN6650B Fibre				Log4j - Security Vulnerability	munica- tion		
	Channel				CVE-2021-44228	Cross		
	Switch				C V L-2021-44220	Refer-		
	SWITTELL					ence ID:		
						SIK7387		
HPE	HPE		Not		(Revision)	Support		2021-12-12
	B-series		Affected		Apache Software	Com-		
	SN6700B				Log4j - Security	munica-		
	Fibre				Vulnerability	tion		
	Channel Switch				CVE-2021-44228	Cross Refer-		
	SWITCH					ence ID:		
						SIK7387		
IPE	$_{ m HPE}$		Not		(Revision)	Support		2021-12-14
	Customer		Affected		Apache Software	Com-		
	Experience				Log4j - Security	munica-		
	Assurance				Vulnerability	tion		
	(CEA)				CVE-2021-44228	Cross		
						Refer-		
						ence ID: SIK7387		
HPE	HPE		Not		(Revision)	Support		2021-12-12
11 12	Hardware		Affected		Apache Software	Com-		2021-12-12
	Support				Log4j - Security	munica-		
	Manager				Vulnerability	tion		
	plug-in for				CVE-2021-44228	Cross		
	VMware					Refer-		
	vSphere					ence ID:		
	Lifecycle					SIK7387		
	Manager							

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
НРЕ	HPE Home Location Register (HLR/I- HLR)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14
HPE	HPE Infosight for Servers		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
НРЕ	HPE Integrated Home Subscriber Server (I-HSS)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14
HPE	HPE Intelligent Messaging (IM)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14
HPE	HPE Intelligent Network Server (INS)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	HPE Multimedia Services Environment (MSE)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14
HPE	HPE OC Convergent Communi- cations Platform (OCCP)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence 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 Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14
HPE	HPE OC Service Access Controller (OC SAC)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14
HPE	HPE OC Service Controller (OCSC)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence 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 Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14
HPE	HPE OneView		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence 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 Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
НРЕ	HPE OneView Global Dashboard		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
НРЕ	HPE Performance Cluster Manager (HPCM)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
НРЕ	HPE Performance Manager (PM)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14
HPE	HPE Position Determina- tion Entity (PDE)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14
HPE	HPE Secure Identity Broker (SIB)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14
HPE	HPE Service Activator (SA)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14
HPE	HPE Service Gover- nance Framework (SGF)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	HPE Service Or- chestration Manager (SOM)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14
HPE	HPE Service Provisioner (SP)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence 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 Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14
НРЕ	HPE Slingshot		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	HPE Smart Interaction Server (SIS)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	HPE SN3000B Fibre Channel Switch		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence 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 Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	HPE SN8000B 8-Slot SAN Backbone Director Switch		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	HPE SN8600B 4-Slot SAN Director Switch		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	HPE SN8600B 8-Slot SAN Director Switch		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
НРЕ	HPE SN8700B 4-Slot Director Switch		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
НРЕ	HPE SN8700B 8-Slot Director Switch		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	HPE Subscriber, Network, and Appli- cation Policy (SNAP)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14
HPE	HPE Subscription Manager (SM)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14
HPE	HPE Synergy Image Streamer		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	HPE Systems Insight Manager (SIM)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
НРЕ	HPE Telecom Application Server (TAS)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14
НРЕ	HPE Unified Correlation and Au- tomation (UCA)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14
НРЕ	HPE Unified Mediation Bus (UMB)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14
HPE	HPE Unified OSS Console (UOC)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	HPE Unified Topology Manager (UTM)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14
HPE	HPE Universal Identity Repository (VIR)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14
HPE	HPE Universal SLA Manager (uSLAM)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14
HPE	HPE Virtual Connect		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	HPE Virtual Connect Enterprise Manager (VCEM)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	HPE Virtual Provision- ing Gateway (vPGW)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14
НРЕ	HPE Virtual Server En- vironment (VSE)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	HPE Virtual Subscriber Data Man- agement (vSDM)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14
HPE	HPE WebRTC Gateway Controller (WGW)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-14
НРЕ	HPE Wi-Fi Authentica- tion Gateway (WauG)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	Insight Cluster Manage- ment Utility (CMU)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
НРЕ	Integrated Lights-Out (iLO) Amplifier Pack		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	Integrated Lights-Out 4 (iLO 4)	4	Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	Integrated Lights-Out 5 (iLO 5)	5	Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
НРЕ	Integrity BL860c, BL870c, BL890c		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12

Vendor	$Product \qquad Version(s)$	Status Update Available	Vendor Link	Notes Other References	Last Updated
HPE	Integrity Rx2800/Rx2900	Not Affected	(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387	2021-12-12
HPE	Integrity Superdome 2	Not Affected	(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387	2021-12-12
НРЕ	Integrity Superdome X	Not Affected	(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387	2021-12-12
HPE	Intelligent Provisioning	Not Affected	(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387	2021-12-12
HPE	iSUT integrated smart update tool	Not Affected	(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Communication Cross Reference ID: SIK7387	2021-12-12

2021-12-12 2021-12-12
2021 12 12
2021 12 12
2021 12 12
2021 12 12
2021 12 12
2021 12 12
2021 12 12
20121-12-12
2021 12 12
2021-12-12
2021-12-12

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	NS-T0977- SCHEMA VALIDATO)R	Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	OfficeConne	ect	Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
НРЕ	Primera Storage		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	RepoServer part of OPA (on Premises aggregator)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	Resource Aggregator for Open Distributed Infrastruc- ture Managemen	I	Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	RESTful In- terface Too (iLOREST)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	SAT (System Admin Toolkit)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	Scripting Tools for Windows PowerShell (HPEiLOC	mdlets)	Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	SGI MC990 X Server)	Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	SGI UV 2000 Server	-	Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	SGI UV 300, 300H, 300RL, 30EX		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
НРЕ	SGI UV 3000 Server		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	SN8700B 8-Slot Director Switch		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
НРЕ	StoreEasy		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	StoreEver CVTL		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HPE	StoreEver LTO Tape Drives		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
НРЕ	StoreEver MSL Tape Libraries		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	StoreOnce		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	SUM (Smart Update Manager)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
HPE	Superdome Flex 280		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
НРЕ	Superdome Flex Server		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12
НРЕ	UAN (User Access Node)		Not Affected		(Revision) Apache Software Log4j - Security Vulnerability CVE-2021-44228	Support Com- munica- tion Cross Refer- ence ID: SIK7387		2021-12-12

/endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
OLOGIC	Advanced		Affected	No	HOLOGIC	While	12/20/2021
	Workflow				Advisory Link	the	, ,
	Manager				·	Hologic	
	(AWM)					soft-	
						ware	
						itself	
						does	
						not	
						utilize	
						Java/Log4J,	
						the in-	
						stalled	
						APC	
						Power-	
						Chute	
						UPS	
						with	
						Busi-	
						ness	
						Edition	
						v9.5	
						soft-	
						ware	
						in-	
						stalled	
						may.	
						APC is	
						still as-	
						sessing	
						its	
						Power-	
						Chute	
						soft-	
						ware to	
						deter-	
						mine if	
						it is	
						vulnerable.	

Vendor Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
endor Product OLOGIC Unifi Workspace	Version(s)	Status Affected	Update Available No	Vendor Link HOLOGIC Advisory Link	While the Hologic software itself does not utilize Java/Lo the installed APC Power-Chute UPS with Business Edition v9.5 software installed may. APC is still assessing its Power-Chute software to determine if it is		Last Updated 12/20/2021

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
OLOGIC	Faxitron		Affected	No	HOLOGIC	While	12/20/2021
	CT				Advisory Link	the	
	Specimen					Hologic	
	Radiogra-					soft-	
	phy					ware	
	System					itself	
						does	
						not	
						utilize	
						Java/Log4J,	
						there is	
						a	
						utility	
						pro-	
						gram	
						in-	
						stalled	
						that	
						may	
						utilize	
						Java	
						and	
						Log4J. This	
						utility	
						pro-	
						gram does	
						not run	
						on	
						startup	
						and is	
						not re-	
						quired	
						for	
						system	
						opera-	
						tion.	
						Please	
						contact	
						Hologic	
						Service	
						for	
						assis-	
						tance	
						in re-	
						moving	
						this	
						tnis	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
HOLOGIC	Dimensions / 3Dimensions Mammography System		Not Affected	No	HOLOGIC Advisory Link			12/20/2021
HOLOGIC			Not Affected	No	HOLOGIC Advisory Link			12/20/2021
HOLOGIC			Not Affected	No	HOLOGIC Advisory Link			12/20/2021
HOLOGIC	Trident HD Specimen Radiogra- phy System		Not Affected	No	HOLOGIC Advisory Link			12/20/2021
HOLOGIC	SecurView DX Workstation		Not Affected	No	HOLOGIC Advisory Link			12/20/2021
HOLOGIC			Not Affected	No	HOLOGIC Advisory Link			12/20/2021
HOLOGIC	SecurXChange Router		Not Affected	No	HOLOGIC Advisory Link			12/20/2021
HOLOGIC			Not Affected	No	HOLOGIC Advisory Link			12/20/2021
HOLOGIC	Faxitron Specimen Radiogra- phy Systems		Not Affected	No	HOLOGIC Advisory Link			12/20/2021
HOLOGIC			Not Affected	No	HOLOGIC Advisory Link			12/20/2021
HOLOGIC			Not Affected	No	HOLOGIC Advisory Link			12/20/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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			Not Affected	No	HOLOGIC Advisory Link			12/20/2021
Huawei					Huawei Security Notice			
Hubspot I-Net software I2P IBA-AG					Hubspot Notice I-Net Software Statement I2P Statement IBA-AG Statement Ibexa Statement			
IBM	BigFix Compliance		Affected	No	TOCAR DIRECTION			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	BigFix	VM Manager	Affected	No		То		
	Inventory	Tool & SAP Tool				verify if		
						your in-		
						stance		
						is af-		
						fected,		
						go to		
						the lib		
						subdi-		
						rectory		
						of the		
						tool		
							ent/LMT/SAPTOOL	
						and	, , , , , , , , , , , , , , , , , , , ,	
							nt/LMT/VMMAN)	
						and		
						check		
						what		
						version		
						of log4j		
						is in-		
						cluded.		
						Version		
						is in-		
						cluded		
						in the		
						name		
						of the		
ID) (A 1		NT :		A 1	library.		10/15/0001
IBM	Analytics		Not		An update on the			12/15/2021
	Engine		Affected		Apache Log4j			
					CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			
IBM	App		Not		An update on the			12/15/2021
	Configuratio	n	Affected		Apache Log4j			
					CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			
IBM	App		Not		An update on the			12/15/2021
	Connect		Affected		Apache Log4j			
					CVE-2021-44228			
					vulnerability -			
					v dilicianilio,			

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	Block		Not		An update on the			12/15/2021
	Storage		Affected		Apache Log4j			
	Snapshots				CVE-2021-44228			
	for VPC				vulnerability - IBM PSIRT Blog			
IBM	Case		Not		An update on the			12/15/2021
IDM	Manager		Affected		Apache Log4j			12/10/2021
	1,10110801		111100004		CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			
IBM	Certificate		Affected	Yes	An update on the			12/15/2021
	Manager				Apache Log4j			
					CVE-2021-44228			
					vulnerability - IBM PSIRT Blog			
IBM	Client VPN		Not		An update on the			12/15/2021
IDM	for VPC		Affected		An update on the Apache Log4j			12/10/2021
	101 11 0		Tinected		CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			
IBM	Cloud		Not		An update on the			12/15/2021
	Activity		Affected		Apache Log4j			
	Tracker				CVE-2021-44228			
					vulnerability -			
IBM	Cloud		Not		IBM PSIRT Blog			19/15/9091
IDM	Backup		Affected		An update on the Apache Log4j			12/15/2021
	Баскир		Affected		CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			
IBM	Cloud		Not		An update on the			12/15/2021
	Monitoring		Affected		Apache Log4j			
					CVE-2021-44228			
					vulnerability -			
IDM	C1 1		A.C 1	V	IBM PSIRT Blog			10/15/0001
IBM	Cloud Object		Affected	Yes	An update on the Apache Log4j			12/15/2021
	Storage				CVE-2021-44228			
	Storage				vulnerability -			
					IBM PSIRT Blog			
IBM	Cloud		Affected	Yes	An update on the			12/15/2021
	Object				Apache Log4j			•
	Storage				CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	Cloudant		Affected	Yes	An update on the			12/15/2021
					Apache Log4j			
					CVE-2021-44228			
					vulnerability - IBM PSIRT Blog			
IBM	Code		Not		An update on the			12/15/2021
IDM	Engine		Affected		An update on the Apache Log4j			12/19/2021
	Liigine		Miccica		CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			
IBM	Cognos		Not		An update on the			12/15/2021
	Command		Affected		Apache Log4j			, ,
	Center				CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			
$_{\rm IBM}$	Cognos	10.4.2	Affected	Yes	Security Bulletin:			12/15/2021
	Controller				IBM Cognos			
					Controller 10.4.2			
					IF15: Apache			
					log4j			
					Vulnerability			
					(CVE-2021- 44228)			
IBM	Cognos		Not		An update on the			12/15/2021
.DIVI	Integration		Affected		An update on the Apache Log4j			12/19/2021
	Server		Miccica		CVE-2021-44228			
	DCI VCI				vulnerability -			
					IBM PSIRT Blog			
BM	Compose		Not		An update on the			12/15/2021
	Enterprise		Affected		Apache Log4j			, ,
	•				CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			
$_{\rm IBM}$	Compose		Not		An update on the			12/15/2021
	for		Affected		Apache Log4j			
	Elasticsearch				CVE-2021-44228			
					vulnerability -			
	~		2.7		IBM PSIRT Blog			40.14
IBM	Compose		Not		An update on the			12/15/2021
	for etcd		Affected		Apache Log4j			
					CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	Compose		Not		An update on the			12/15/2021
	for		Affected		Apache Log4j			
	MongoDB				CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			
IBM	Compose		Not		An update on the			12/15/2021
	for MySQL		Affected		Apache Log4j			
					CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			
IBM	Compose		Not		An update on the			12/15/2021
	for		Affected		Apache Log4j			
	${\bf Postgre SQL}$				CVE-2021-44228			
					vulnerability -			
TD3.6	~		37.		IBM PSIRT Blog			10/15/10001
IBM	Compose		Not		An update on the			12/15/2021
	for		Affected		Apache Log4j			
	RabbitMQ				CVE-2021-44228			
					vulnerability -			
TDM	C C		37.		IBM PSIRT Blog			10/15/0001
IBM	Compose		Not		An update on the			12/15/2021
	for Redis		Affected		Apache Log4j CVE-2021-44228			
					vulnerability -			
IBM	Common		Not		IBM PSIRT Blog An update on the			12/15/2021
IDM	Compose for		Affected		An update on the Apache Log4j			12/13/2021
	RethinkDB		Affected		CVE-2021-44228			
	пенникръ				vulnerability -			
					IBM PSIRT Blog			
IBM	Compose		Not		An update on the			12/15/2021
IDM	for		Affected		Apache Log4j			12/10/2021
	ScyllaDB		Tinected		CVE-2021-44228			
	осупарь				vulnerability -			
					IBM PSIRT Blog			
IBM	Container		Affected	Yes	An update on the			12/15/2021
15111	Registry		Tillectica	100	Apache Log4j			12/10/2021
	10081001				CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			
IBM	Container		Affected	Yes	An update on the			12/15/2021
	Security				Apache Log4j			, ,
	Services				CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			

Vendor	$Product \qquad Version(s)$	Status	Update Available	Vendor Link	Notes Other References	Last Updated
IBM	Content Delivery Network	Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog		12/15/2021
IBM	Continuous Delivery	Affected	Yes	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog		12/15/2021
IBM	Copy Services Manager	Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog		12/15/2021
IBM	Databases for DataStax	Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog		12/15/2021
IBM	Databases for EDB	Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog		12/15/2021
IBM	Databases for Elasticsearch	Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog		12/15/2021
IBM	Databases for etcd	Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog		12/15/2021
IBM	Databases for MongoDB	Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog		12/15/2021
IBM	Databases for PostgreSQL	Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog		12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	Databases for Redis		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability -			12/15/2021
IBM	Datapower Gateway		Not Affected		IBM PSIRT Blog An update on the Apache Log4j CVE-2021-44228			12/15/2021
IBM	Dedicated Host for		Not Affected		vulnerability - IBM PSIRT Blog An update on the Apache Log4j			12/15/2021
	VPC		Affected		CVE-2021-44228 vulnerability - IBM PSIRT Blog			
IBM	Direct Link Connect		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Direct Link Connect on Classic		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Direct Link Dedicated (2.0)		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Direct Link Dedicated Hosting on Classic		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Direct Link Dedicated on Classic		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Direct Link Exchange on Classic		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021

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

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	Hyper Protect DBaaS for MongoDB		Affected	Yes	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Hyper Protect DBaaS for PostgreSQL		Affected	Yes	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Hyper Protect Virtual Server		Affected	Yes	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	i2 Analyst's Notebook		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	i2 Base		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	IBM Application Runtime Expert for i		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	IBM Backup, Recovery and Media Services for i		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	IBM Db2 Mirror for i		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	IBM HTTP Server		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021

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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	IBM		Not		An update on the			12/15/2021
	Sterling		Affected		Apache Log4j			
	Con-				CVE-2021-44228			
	nect:Direct				vulnerability -			
	for				IBM PSIRT Blog			
	OpenVMS				O			
IBM	IBM		Not		An update on the			12/15/2021
	Sterling		Affected		Apache Log4j			, -, -
	Con-				CVE-2021-44228			
	nect:Express				vulnerability -			
	for				IBM PSIRT Blog			
	Microsoft				IDM I DIRT DIOS			
	Windows							
IBM	IBM		Not		An update on the			12/15/2021
IDM			Affected					12/13/2021
	Sterling		Affected		Apache Log4j			
	Con-				CVE-2021-44228			
	nect:Express				vulnerability -			
TDM (for UNIX		3.7		IBM PSIRT Blog			10/12/2021
IBM	IBM		Not		An update on the			12/15/2021
	Sterling		Affected		Apache Log4j			
	Con-				CVE-2021-44228			
	nect:Express				vulnerability -			
	for z/OS				IBM PSIRT Blog			
IBM	Instana Agent	Timestamp lower than 12-11-2021	Affected	Yes	Status Instana			12/14/2021
IBM	Internet	12 11 2021	Affected	Yes	An update on the			12/15/2021
1171/1	Services		Amedeu	100	An update on the Apache Log4j			12/10/2021
	Det Arces				CVE-2021-44228			
					vulnerability -			
IDM	17		NI - 4		IBM PSIRT Blog			10/15/0001
IBM	Key		Not		An update on the			12/15/2021
	Lifecyle		Affected		Apache Log4j			
	Manager				CVE-2021-44228			
	for z/OS				vulnerability -			
					IBM PSIRT Blog			
IBM	Key		Not		An update on the			12/15/2021
	Protect		Affected		Apache Log4j			
					CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			
IBM	Knowledge		Affected	Yes	An update on the			12/15/2021
	Studio				Apache Log4j			
					CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			

Vendor	Product Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
IBM	Kubernetes Service	Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog		12/15/2021
IBM	Load Balancer for VPC	Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog		12/15/2021
IBM	Log Analysis	Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog		12/15/2021
IBM	Managed VMware Service	Affected	Yes	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog		12/15/2021
IBM	Management Extender for VMware vCenter	Affected	No	Ü		
IBM	Mass Data Migration	Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog		12/15/2021
IBM	Maximo EAM SaaS	Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog		12/15/2021
IBM	Message Hub	Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog		12/15/2021
IBM	MQ Appliance	Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog		12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	MQ on IBM Cloud		Not Affected		An update on the Apache Log4j			12/15/2021
	IDM Cloud		Affected		CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			
IBM	Natural		Affected	Yes	An update on the			12/15/2021
	Language				Apache Log4j			
	Understandin	ng			CVE-2021-44228			
					vulnerability -			
TD	0		37		IBM PSIRT Blog			10/17/0001
IBM	OmniFind		Not		An update on the			12/15/2021
	Text		Affected		Apache Log4j CVE-2021-44228			
	Search Server for				vulnerability -			
	DB2 for i				IBM PSIRT Blog			
IBM	OPENBMC		Not		An update on the			12/15/2021
115111	OT EITEIN		Affected		Apache Log4j			12/10/2021
					CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			
IBM	Planning	>2.0.57	Affected	Yes	Security Bulletin:			12/15/2021
	Analytics				IBM Planning			
	Workspace				Analytics 2.0:			
					Apache log4j			
					Vulnerability			
					(CVE-2021- 44228)			
IBM	Power	V9.2.950.0 &	Affected	Yes	Security Bulletin:			12/15/2021
IDM	HMC	V10.1.1010.0	Affected	105	Vulnerability in			12/10/2021
	111110	V 10.1.1010.0			Apache Log4j			
					(CVE-2021-			
					44228) affects			
					Power HMC			
IBM	PowerSC		Not		An update on the			12/15/2021
			Affected		Apache Log4j			
					CVE-2021-44228			
					vulnerability -			
IDM	D 173.6		NT /		IBM PSIRT Blog			10/15/0001
IBM	PowerVM		Not		An update on the			12/15/2021
	Hypervisor		Affected		Apache Log4j CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			
					IBM PSIKT Blog			

lor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
	PowerVM		Not		An update on the			12/15/2021
	VIOS		Affected		Apache Log4j			
					CVE-2021-44228			
					vulnerability -			
	QRadar		Not		IBM PSIRT Blog An update on the			12/15/2021
-	Advisor		Affected		An update on the Apache Log4j			12/19/2021
	114 11501		Hillococa		CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			
	Qradar		Not		An update on the			12/15/2021
	Network		Affected		Apache Log4j			
	Threat				CVE-2021-44228			
	Analytics				vulnerability -			
	OD - 1		Not		IBM PSIRT Blog			10/17/0001
	QRadar SIEM		Affected		An update on the Apache Log4j			12/15/2021
	SIEW		Affected		CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			
	Quantum		Not		An update on the			12/15/2021
	Services		Affected		Apache Log4j			
					CVE-2021-44228			
					vulnerability -			
	D 1		37.		IBM PSIRT Blog			10/15/0001
	Rational		Not Affected		An update on the			12/15/2021
	Developer for AIX		Апестеа		Apache Log4j CVE-2021-44228			
	and Linux				vulnerability -			
	and Dinas				IBM PSIRT Blog			
	Rational		Not		An update on the			12/15/2021
	Developer		Affected		Apache Log4j			
	for i				CVE-2021-44228			
					vulnerability -			
	D 1114		NT 4		IBM PSIRT Blog			10/17/0001
	Red Hat OpenShift		Not Affected		An update on the Apache Log4j			12/15/2021
	on IBM		Affected		CVE-2021-44228			
	Cloud				vulnerability -			
	01044				IBM PSIRT Blog			
	Resilient		Under					
			Investigation	on				
	Robotic		Not		An update on the			12/15/2021
	Process		Affected		Apache Log4j			
	Automation				CVE-2021-44228			
					vulnerability -			

Vendor	${\bf Product} \qquad {\bf Version(s)}$	Status Update Available	Vendor Link Notes Other References	Last Updated
IBM	SAN Volume Controller and Storwize	Not Affected	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog	12/15/2021
IBM	Family Satellite Infrastruc- ture Service	Not Affected	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog	12/15/2021
IBM	Schematics	Not Affected	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog	12/15/2021
IBM	Secrets Manager	Not Affected	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog	12/15/2021
IBM	Secure Gateway	Not Affected	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog	12/15/2021
IBM	Server Automation	Affected No	IBM TORKE BIOS	
IBM	Spectrum Archive Library Edition	Not Affected	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog	12/15/2021
IBM	Spectrum Discover	Not Affected	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog	12/15/2021
IBM	Spectrum Protect Client Man- agement Service	Not Affected	An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog	12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	Spectrum		Not		An update on the			12/15/2021
	Protect for		Affected		Apache Log4j			
	Databases:				CVE-2021-44228			
	Data				vulnerability -			
	Protection				IBM PSIRT Blog			
	for Oracle							
IBM	Spectrum		Not		An update on the			12/15/2021
	Protect for		Affected		Apache Log4j			, ,
	Databases:				CVE-2021-44228			
	Data				vulnerability -			
	Protection				IBM PSIRT Blog			
	for SQL							
IBM	Spectrum		Not		An update on the			12/15/2021
	Protect for		Affected		Apache Log4j			, ,
	Enterprise				CVE-2021-44228			
	Resource				vulnerability -			
	Planning				IBM PSIRT Blog			
BM	Spectrum		Not		An update on the			12/15/2021
	Protect for		Affected		Apache Log4j			, ,
	Mail: Data				CVE-2021-44228			
	Protection				vulnerability -			
	for Domino				IBM PSIRT Blog			
BM	Spectrum		Not		An update on the			12/15/2021
	Protect for		Affected		Apache Log4j			, ,
	Mail: Data				CVE-2021-44228			
	Protection				vulnerability -			
	for				IBM PSIRT Blog			
	Exchange							
BM	Spectrum		Not		An update on the			12/15/2021
	Protect for		Affected		Apache Log4j			, ,
	Workstations	S			CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			
BM	Spectrum		Not		An update on the			12/15/2021
	Protect for		Affected		Apache Log4j			, ,
	z/OS USS				CVE-2021-44228			
	Client and				vulnerability -			
	API				IBM PSIRT Blog			
BM	Spectrum		Not		An update on the			12/15/2021
	Protect		Affected		Apache Log4j			, ,
	Plus Db2				CVE-2021-44228			
	Agent				vulnerability -			
	-				IBM PSIRT Blog			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	Spectrum Protect Plus Exchange Agent		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Spectrum Protect Plus File Systems Agent		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Spectrum Protect Plus MongoDB Agent		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Spectrum Protect Plus O365 Agent		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Spectrum Protect Server		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Spectrum Protect Snapshot for UNIX		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Spectrum Protect Snapshot for UNIX		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	SQL Query		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Sterling Gentran		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	Sterling Order Management		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Sterling Transfor- mation Extender Pack for ACORD		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Sterling Transfor- mation Extender Pack for Financial Services		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Sterling Transfor- mation Extender Pack for FIX		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Sterling Transfor- mation Extender Pack for NACHA		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Sterling Transfor- mation Extender Pack for PeopleSoft		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Sterling Transfor- mation Extender Pack for SAP R/3		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 Transfor- mation		Not Affected		An update on the Apache Log4j CVE-2021-44228			12/15/2021
	Extender Pack for SEPA				vulnerability - IBM PSIRT Blog			
IBM	Sterling		Not		An update on the			12/15/2021
	Transfor-		Affected		Apache Log4j			
	mation				CVE-2021-44228			
	Extender Pack for				vulnerability - IBM PSIRT Blog			
	Siebel				Bold falkt blog			
IBM	Sterling		Not		An update on the			12/15/2021
	Transfor-		Affected		Apache Log4j			, ,
	mation				CVE-2021-44228			
	Extender				vulnerability -			
	Pack for				IBM PSIRT Blog			
TD) (SWIFT		37		A 1			10/17/0001
IBM	Sterling Transfor-		Not Affected		An update on the			12/15/2021
	mation		Affected		Apache Log4j CVE-2021-44228			
	Extender				vulnerability -			
	Packs for				IBM PSIRT Blog			
	EDI				O			
$_{\rm IBM}$	Sterling		Not		An update on the			12/15/2021
	Transfor-		Affected		Apache Log4j			
	mation				CVE-2021-44228			
	Extender				vulnerability -			
	Packs for Healthcare				IBM PSIRT Blog			
IBM	Sterling		Not		An update on the			12/15/2021
115111	Transfor-		Affected		Apache Log4j			12/10/2021
	mation				CVE-2021-44228			
	Extender				vulnerability -			
	Trading				IBM PSIRT Blog			
	Manager							
IBM	Storage		Not		An update on the			12/15/2021
	TS1160		Affected		Apache Log4j			
					CVE-2021-44228			
					vulnerability - IBM PSIRT Blog			
IBM	Storage		Not		An update on the			12/15/2021
TDM	TS2280		Affected		An apaate on the Apache Log4j			12/10/2021
	1.2 -1 00		111100004		CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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 Virtualiza- tion Engine TS7700		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Tape System Library Manager		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	TDMF for zOS		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Total Storage Service Console (TSSC) / TS4500 IMC		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Transit Gateway		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021
IBM	Tririga Anywhere		Not Affected		An update on the Apache Log4j CVE-2021-44228 vulnerability - IBM PSIRT Blog			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	TS4300		Not		An update on the			12/15/2021
			Affected		Apache Log4j			
					CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			
IBM	Urbancode		Not		An update on the			12/15/2021
	Deploy		Affected		Apache Log4j			
					CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			
IBM	Virtual		Not		An update on the			12/15/2021
	Private		Affected		Apache Log4j			
	Cloud				CVE-2021-44228			
					vulnerability -			
TDM	3 7: 4 1		NT /		IBM PSIRT Blog			10/17/0001
IBM	Virtual		Not		An update on the			12/15/2021
	Server for Classic		Affected		Apache Log4j CVE-2021-44228			
	Classic				vulnerability -			
					IBM PSIRT Blog			
IBM	Virtualizatio	n	Not		An update on the			19/15/2021
IDM	Manage-	111	Affected		An update on the Apache Log4j			12/19/2021
	ment		Miccica		CVE-2021-44228			
	Interface				vulnerability -			
	menaec				IBM PSIRT Blog			
IBM	VMware		Affected	Yes	An update on the			12/15/2021
121.1	Solutions		111100000	100	Apache Log4j			12/10/2021
					CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			
IBM	VMware		Affected	Yes	An update on the			12/15/2021
	vCenter				Apache Log4j			, ,
	Server				CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			
IBM	VMware		Affected	Yes	An update on the			12/15/2021
	vSphere				Apache Log4j			
					CVE-2021-44228			
					vulnerability -			
TD3.6			2.5		IBM PSIRT Blog			and the state of
IBM	VPN for		Not		An update on the			12/15/2021
	VPC		Affected		Apache Log4j			
					CVE-2021-44228			
					vulnerability -			
					IBM PSIRT Blog			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IBM	vRealize Operations and Log		Affected	Yes	An update on the Apache Log4j CVE-2021-44228			12/15/2021
	Insight				vulnerability - IBM PSIRT Blog			
IBM	Workload		Not		An update on the			12/15/2021
	Automation		Affected		Apache Log4j			, -, -
					CVE-2021-44228			
					vulnerability - IBM PSIRT Blog			
ICONICS	All		Not		ICONICS			12/21/2021
10011100	1111		Affected		Advisory Link			12/21/2021
IFS					IFS Bulletin			
IGEL					IGEL Statement			
Ignite					Ignite Realtime			
Realtime					Statement			
iGrafx					iGrafx Statement			
Illuminate	d				Illuminated			
Cloud					Cloud Statement			
Illumio	C-VEN		Not		Illumio KB			12/16/2021
T11 .	CT T		Affected		article			10/10/201
Illumio	CLI		Not		Illumio KB			12/16/2021
т11 •	C1 10		Affected		article			10/10/0001
Illumio	CloudSecure		Not Affected		Illumio KB article			12/16/2021
Illumio	Core		Not		Illumio KB			12/16/2021
mumo	on-premise		Affected		article			12/10/2021
	PCE		Miccica		articic			
Illumio	Core SaaS		Not		Illumio KB			12/16/2021
	PCE		Affected		article			//
Illumio	Edge SaaS		Not		Illumio KB			12/16/2021
	$\overrightarrow{\text{PCE}}$		Affected		article			, ,
Illumio	Edge-		Not		Illumio KB			12/16/2021
	CrowdStrike		Affected		article			
Illumio	Flowlink		Not		Illumio KB			12/16/2021
			Affected		article			
Illumio	Kubelink		Not		Illumio KB			12/16/2021
			Affected		article			
Illumio	NEN		Not		Illumio KB			12/16/2021
			Affected		article			
Illumio	QRadar		Not		Illumio KB			12/16/2021
	App		Affected		article			
Illumio	Splunk		Not		Illumio KB			12/16/2021
	App		Affected		article			
Illumio	VEN		Not		Illumio KB			12/16/2021
			Affected		article			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
IManage					IManage			
_					Statement			
Imperva					Imperva			
т 1					Statement			
Inductive					Inductive			
Automatic	on				Automation			
Industrial	Defenden				Statement IndustrialDefender			
maustriai.	Defender				Statement			
infinidat					infinidat			
IIIIIIIIIIIIII					Statement			
InfluxData	a				InfluxData			
manbaa					Statement			
Infoblox					Infoblox			
					Statement			
Informatio	ca				Informatica			
					Statement			
Instana					Instana			
					Statement			
Instructur	e				Instructure			
					Statement			
Intel	Audio De-		Affected	No	Intel Advisory			12/16/2021
	velopment							
	Kit							
Intel	Datacenter		Affected	No	Intel Advisory			12/16/2021
T . 1	Manager		1.00		T . 1 4 1 4			10/10/2021
Intel	oneAPI		Affected		Intel Advisory			12/16/2021
	sample							
	browser							
	plugin for Eclipse							
Intel	System		Affected		Intel Advisory			12/16/2021
111001	Debugger		Miccica		inter ravisory			12/10/2021
Intel	Secure		Affected		Intel Advisory			12/16/2021
111001	Device		111100004		111001 114 (1501)			12/10/2021
	Onboard							
Intel	Genomics		Affected		Intel Advisory			12/16/2021
	Kernel				·			, ,
	Library							
Intel	System		Affected		Intel Advisory			12/16/2021
	Studio							
Intel	Computer		Affected		Intel Advisory			12/16/2021
	Vision							
	Annotation							
	Tool							
	maintained							
	by Intel							

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Intel	Sensor Solution Firmware Develop- ment Kit		Affected		Intel Advisory		12/16/2021
Internet Systems Consortium	ISC DHCP, aka dhcpd m(ISC)	All	Not Affected	N/A	ISC Open Source and Log4J	no JAVA Code	12/17/2021
Internet Systems Consortium	Kea DHCP	All	Not Affected	N/A	ISC Open Source and Log4J	no JAVA Code	12/17/2021
Internet Systems Consortium InterSystem	BIND 9 m(ISC)	All	Not Affected	N/A	ISC Open Source and Log4J InterSystems Statement	no JAVA Code	12/17/2021
Intland	codebeamer	<= 20.11-SP11, <= 21.09-SP3	Affected	Some releases	Apache Log4j vulnerability and fixes	A fix has been re- leased for 20.11 and 21.09, but not yet for 21.04	
IPRO iRedMail	Netgovern				iRedMail Statement		
Ironnet	NE				Ironnet Security Notification ISLONLINE Statement		
Ivanti Jamasoftw	are				Ivanti Statement Jamasoftware Statement		
Jamf	Jamf Pro	10.31.0 - 10.34.0	Affected	Yes	Mitigating the Apache Log4j 2 Vulnerability		
Jaspersoft Jedox					Jaspersoft Statement Jedox Statement		
Jenkins	CI/CD Core		Not Affected		Jedox Statement		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Jenkins	Plugins		Some affected, some fixed, most unaffected. See issue tracker	Some	Announcement, issue tracker	Instruction to test your installations in announcement	ons	2021-12-16
JetBrains	IntelliJ platform based IDEs (AppCode, CLion, DataGrip, DataSpell, GoLand, IntelliJ IDEA Ultimate/Comm PhpStorm, PyCharm Profes- sional/Comm		Not Affected		JetBrains Blog Post			
JetBrains	Rider, RubyMine, WebStorm) All .NET tools (ReSharper, Rider, ReSharper C++, dotTrace, dotMemory, dotCover, dotPeek)	Unknown	Not Affected		JetBrains Blog Post			
JetBrains	ToolBox	Unknown	Not Affected		JetBrains Blog Post			
JetBrains	TeamCity	Unknown	Not Affected		JetBrains Blog Post			
JetBrains	Hub	2021.1.14080	Fixed		JetBrains Blog Post			
JetBrains JetBrains	YouTrack Standalone YouTrack InCloud	2021.4.35970 Unknown	Fixed Fixed		JetBrains Blog Post JetBrains Blog Post			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
JetBrains	Datalore	Unknown	Not		JetBrains Blog			
			Affected		Post			
JetBrains	Space	Unknown	Not		JetBrains Blog			
			Affected		Post			
Jetbrains	Code With	Unknown	Fixed		JetBrains Blog			
	Me				Post			
JetBrains	Gateway	Unknown	Not		JetBrains Blog			
			Affected		Post			
JetBrains	Kotlin	Unknown	Not		JetBrains Blog			
			Affected		Post			
JetBrains	Ktor	Unknown	Not		JetBrains Blog			
			Affected		Post			
JetBrains	MPS	Unknown	Not		JetBrains Blog			
			Affected		Post			
JetBrains	Floating	30211	Fixed		JetBrains Blog			
	license				Post			
	server							
JetBrains	UpSource	2020.1.1952	Fixed		JetBrains Blog			
					Post			
JFROG					JFROG			
					Statement			
Jitsi					Jitsi Advisory			
Jitterbit					Jitterbit			
					Statement			
jPOS	(ISO-8583)	Unknown	Not		source			
	bridge		Affected					
Johnson	C • CURE-	2.90.x (all 2.90	Not		Johnson Controls			12/21/2021
Controls	9000	versions)	Affected		Advisory Link			, ,
Johnson	C • CURE-	2.80.x (all 2.80	Not		Johnson Controls			12/21/2021
Controls	9000	versions)	Affected		Advisory Link			, ,
Johnson	C • CURE-	2.70 (All	Not		Johnson Controls			12/21/2021
Controls	9000	versions)	Affected		Advisory Link			, ,
Johnson	C • CURE-	2.60 (All	Not		Johnson Controls			12/21/2021
Controls	9000	versions)	Affected		Advisory Link			, ,
Johnson	victor	5.x	Not		Johnson Controls			12/21/2021
Controls			Affected		Advisory Link			, ,
Johnson	victor/	3.81.x / victor	Not		Johnson Controls			12/21/2021
Controls	C • CURE-	5.4.1 /	Affected		Advisory Link			/ / -
	9000	C • CURE-9000			J. C.			
	Unified	2.80						
Johnson	victor/	3.91.x / victor	Not		Johnson Controls			12/21/2021
Controls	C • CURE-	5.6.1 /	Affected		Advisory Link			/ / -
	9000	C • CURE-9000			<i>J</i>			
	Unified	2.90						
Johnson	Metasys	All versions	Not		Johnson Controls			12/21/2021
		1111 (01010110						12/21/2021
Controls	Products		Affected		Advisory Link			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Johnson	Facility	14.x	Not		Johnson Controls			12/21/2021
Controls	Explorer		Affected		Advisory Link			
ohnson	CEM	All versions	Not		Johnson Controls			12/21/2021
Controls	AC2000		Affected		Advisory Link			
Johnson	CEM	All versions	Not		Johnson Controls			12/21/2021
Controls	Hardware		Affected		Advisory Link			, ,
	Products				Ţ.			
Johnson	Illustra	All versions	Not		Johnson Controls			12/21/2021
Controls	Cameras		Affected		Advisory Link			, ,
Johnson	Illustra	All versions	Not		Johnson Controls			12/21/2021
Controls	Insight		Affected		Advisory Link			7 7
Johnson	Tyco AI	All versions	Not		Johnson Controls			12/21/2021
Controls			Affected		Advisory Link			, ,
Johnson	DLS	All versions	Not		Johnson Controls			12/21/2021
Controls			Affected		Advisory Link			, ,
Johnson	Entrapass	All versions	Not		Johnson Controls			12/21/2021
Controls	P		Affected		Advisory Link			,,
Johnson	CloudVue	All versions	Not		Johnson Controls			12/21/2021
Controls	Web	TIII VOIDIOILO	Affected		Advisory Link			1-/-1/
Johnson	CloudVue	All versions	Not		Johnson Controls			12/21/2021
Controls	Gateway	THE VOIDIONS	Affected		Advisory Link			12/21/2021
Johnson	Qolsys IQ	All versions	Not		Johnson Controls			12/21/2021
Controls	Panels	THE VOIDIONS	Affected		Advisory Link			12/21/2021
Johnson	PowerSeries	All versions	Not		Johnson Controls			12/21/2021
Controls	NEO	THI VOIDIONS	Affected		Advisory Link			12/21/2021
Johnson	PowerSeries	All versions	Not		Johnson Controls			12/21/2021
Controls	Pro	THI VOIDIONS	Affected		Advisory Link			12/21/2021
Johnson	Sur-Gard	All versions	Not		Johnson Controls			12/21/2021
Controls	Receivers	7111 VCISIONS	Affected		Advisory Link			12/21/2021
Johnson	VideoEdge	5.x	Not		Johnson Controls			12/21/2021
Controls	VidcoLdge	0.A	Affected		Advisory Link			12/21/2021
Johnson	exacqVision	All versions	Not		Johnson Controls			12/21/2021
Controls	Server	1111 (01510115	Affected		Advisory Link			12/21/2021
Johnson	exacqVision	All versions	Not		Johnson Controls			12/21/2021
Controls	Client	1111 (01510115	Affected		Advisory Link			12/21/2021
Johnson	exacqVision	All versions	Not		Johnson Controls			12/21/2021
Controls	WebService	1111 VOISIONS	Affected		Advisory Link			12/21/2021
Johnson	BCPro	All versions	Not		Johnson Controls			12/21/2021
Controls	DOLLO	1111 VOIDIOHD	Affected		Advisory Link			12/21/2021
Johnson	iSTAR	All versions	Not		Johnson Controls			12/21/2021
Controls	DIAI	All versions	Affected		Advisory Link			14/41/4041
			Allected		Journeyx			
Journyx					Statement			
Lumn					Jump Desktop			
Jump					Statement			
Desktop								
Juniper					Juniper Networks			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Justice					Justice Systems			
Systems					Support			
X15t					K15t Statement			
16					K6 Statement			
Carakun					Karakun			
					Statement			
aseya					Kaseya			
					Vulnerability			
					Assessment			
eeper					Keeper Security			
ecurity					Notice			
EMP					KEMP Support			
EMP 2					KEMP 2			
EMP 2								
c					Support			
ofax					Kofax Product			
					Information			
onica					Konica Minolta			
Iinolta					Support			
ronos					Kronos UKG			
KG					Statement			
yberna					Kyberna			
					Statement			
-Soft					L-Soft Info			
3Harris					L3Harris			
Seospatial					Geospatial			
ancom					Lancom Systems			
ystems					General Security			
5001115					Information			
answeeper					Lansweeper			
лыжеерег					Information			
aserfiche					Laserfiche			
asernene					Product			
					Information			
4D								
astPass					LastPass			
					Information			
aunchDark	ĸly				LaunchDarkly			
					Statement			
eanix					Leanix			
					Statement			
	Aperio AT2	2	Not		Leica			12/21/2021
BIOSYSTE	MS		Affected		BIOSYSTEMS			•
					Advisory Link			
eica	Aperio AT2	?	Not		Leica			12/21/2021
IOSYSTE			Affected		BIOSYSTEMS			, , -
			111100000		Advisory Link			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Leica	Aperio CS2		Not		Leica			12/21/2021
BIOSYST	EMS		Affected		BIOSYSTEMS			
					Advisory Link			
eica	Aperio		Not		Leica			12/21/2021
IOSYST	E MS lide		Affected		BIOSYSTEMS			
	Manager				Advisory Link			
ica	Aperio GT		Not		Leica			12/21/2021
OSYST	E M5 0		Affected		BIOSYSTEMS			
					Advisory Link			
ica	Aperio GT		Not		Leica			12/21/2021
OSYST	E M5 0 DX		Affected		BIOSYSTEMS			
					Advisory Link			
ica	Aperio		Not		Leica			12/21/2021
OSYST	E MS ageScope		Affected		BIOSYSTEMS			
					Advisory Link			
ca	Aperio Im-		Not		Leica			12/21/2021
)SYST	E M§ eScope		Affected		BIOSYSTEMS			
	DX				Advisory Link			
ca	Aperio LV1		Not		Leica			12/21/2021
DSYST	EMS		Affected		BIOSYSTEMS			
					Advisory Link			
ca	Aperio		Under		Leica			12/21/2021
SYST	EMSAM DX		Investigat	ion	BIOSYSTEMS			
	Server For				Advisory Link			
	GT 450 DX							
a	Aperio		Under		Leica			12/21/2021
3YST	E MS anner		Investigat	ion	BIOSYSTEMS			
	Adminis-				Advisory Link			
	tration							
	Manager							
	(SAM)							
	Server for							
	GT 450							
ica	Aperio		Not		Leica			12/21/2021
OSYST	EMSERSA		Affected		BIOSYSTEMS			
					Advisory Link			
ca	Aperio		Not		Leica			12/21/2021
)SYST	EM % ebViewer		Affected		BIOSYSTEMS			
	DX				Advisory Link			, .
ica	BOND-		Not		Leica			12/21/2021
/\ax/am	EMASDVANCE		Affected		BIOSYSTEMS			
J5151.					Advisory Link			
ica	BOND		Not		Leica			12/21/2021
ca	BOND E MS ntroller		Not Affected		Leica BIOSYSTEMS Advisory Link			12/21/2021

Affected BIOSYSTEMS	Vendor Product	t Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Advisory Link		III						12/21/2021
Affected BOND Not	BIOSYSTEMS		Affected					
BIOSYSTEMS								
Advisory Link								12/21/2021
Action	BIOSYSTEM \\$ AX		Affected					
Affected BIOSYSTEMS Affected BIOSYSTEMS Advisory Link Leica BIOSYSTEMS Leica BIOSYSTEMS Leica BIOSYSTEMS Leica								
Advisory Link		RX						12/21/2021
Leica BOND Not Leica BIOSYSTEMS Leica Le	BIOSYSTEMS		Affected					
### Affected BIOSYSTEMS ### Advisory Link	T. DOMB		37 .					10/01/0001
Advisory Link								12/21/2021
Leica CEREBRO	BIOSYSTEMSXm		Affected					
Investigation	I.: CEDED	DD()	II J					10 /01 /0001
Advisory Link		SKO						12/21/2021
Leica CytoVision Not Leica 12/21/2021 BIOSYSTEMS Affected BIOSYSTEMS 12/21/2021 Leica HistoCore Not Leica 12/21/2021 BIOSYSTEMSEARL Affected BIOSYSTEMS 12/21/2021 Leica HistoCore Not Leica 12/21/2021 BIOSYSTEMSEASUS Affected BIOSYSTEMS 12/21/2021 BIOSYSTEMSEASUS Affected BIOSYSTEMS 12/21/2021 BIOSYSTEMSEASUS Affected BIOSYSTEMS 12/21/2021 BIOSYSTEMSECASUS Affected BIOSYSTEMS 12/21/2021 BIOSYSTEMSECASUS Affected BIOSYSTEMS 12/21/2021 BIOSYSTEMSECASUS Affected BIOSYSTEMS 12/21/2021 BIOSYSTEMSECATA Affected BIOSYSTEMS 12/21/2021 BIOSYSTEMSECATA Affected BIOSYSTEMS 12/21/2021 BIOSYSTEMSEASUS Affected BIOSYSTEMS 12/21/2021 BIOSYSTEMSEASUS Affected BIOSYSTEMSEASUS 12/21/2021	DIOSISIEMS		mvestigati	.011				
### Affected ### Affected ### BIOSYSTEMS ### Advisory Link ### Affected ### Affected ### Affected ### Advisory Link ### Affected ### Advisory Link #### Advisory Link ### Advisory Link ### Advisory Link #### Advisory Link ### Advisory Link ### Adviso	Loico CytoVic	sion	Not		v			19/91/9091
Advisory Link		SIOII						12/21/2021
Leica HistoCore Not Leica 12/21/2021 3IOSYSTEMBSARL Affected BIOSYSTEMS Leica HistoCore Not Leica 12/21/2021 BIOSYSTEMBSGASUS Affected BIOSYSTEMS 12/21/2021 BIOSYSTEMS Affected BIOSYSTEMS 12/21/2021 BIOSYSTEMS Affected BIOSYSTEMS 12/21/2021 BIOSYSTEMS Not Leica 12/21/2021 BIOSYSTEMS Affected BIOSYSTEMS 12/21/2021 BIOSYSTEMS Not Leica 12/21/2021 BIOSYSTEMS Advisory Link 12/21/2021 BIOSYSTEMS	DIOSISIEMS		Affected					
BIOSYSTEMS Advisory Link	Laica HistoCo	nro.	Not					19/91/9091
Advisory Link Leica HistoCore Not Leica Leica 12/21/2021								12/21/2021
Leica HistoCore Not Leica 12/21/2021 BIOSYSTEMSEGASUS Affected BIOSYSTEMS Leica HistoCore Not Leica 12/21/2021 BIOSYSTEMSECTRA Affected BIOSYSTEMS 12/21/2021 Leica HistoCore Not Leica 12/21/2021 BIOSYSTEMSECTRA Affected BIOSYSTEMS 12/21/2021 BIOSYSTEMSFIRIT ST Affected BIOSYSTEMS 12/21/2021 BIOSYSTEMSFIRIT ST Affected BIOSYSTEMS 12/21/2021 BIOSYSTEMSFRING Affected BIOSYSTEMS 12/21/2021 BIOSYSTEMSPRING Affected BIOSYSTEMS 12/21/2021 Leica Leica 12/21/2021 BIOSYSTEMSPRING Affected BIOSYSTEMS 12/21/2021		1	Ameeded					
Affected	Leica HistoCo	ore	Not					12/21/2021
Advisory Link Leica Leica 12/21/2021								12/21/2021
Leica HistoCore Not Leica 12/21/2021 BIOSYSTEMS Affected BIOSYSTEMS CV Advisory Link Leica HistoCore Not BIOSYSTEMS Advisory Link Leica HistoCore Not BIOSYSTEMS HistoCore Not BIOSYSTEMS Advisory Link Leica HistoCore Not BIOSYSTEMS HistoCore Not BIOSYSTEMS Advisory Link Leica HistoCore Not BIOSYSTEMS HistoCore Not BIOSYSTEMS HistoCore Not BIOSYSTEMS HistoCore Not BIOSYSTEMS HistoCore Not Leica Leica 12/21/2021 BIOSYSTEMS HistoCore	DIODIDIEM DOIL	700	Tillocood					
Affected BIOSYSTEMS Advisory Link Leica Leic	Leica HistoCo	ore	Not					12/21/2021
CV								1 1 -
Leica HistoCore Not Leica 12/21/2021 BIOSYSTEMSPECTRA Affected BIOSYSTEMS 2 ST Advisory Link 12/21/2021 Leica HistoCore Not Leica 12/21/2021 BIOSYSTEMSPRING Affected BIOSYSTEMS 12/21/2021 BIOSYSTEMSPRING Affected BIOSYSTEMS 12/21/2021 BIOSYSTEMSPRING Not Leica 12/21/2021 BIOSYSTEMSPRING Advisory Link 12/21/2021 BIOSYSTEMSPRING Affected BIOSYSTEMS BIOSYSTEMS 12/21/2021 BIOSYSTEMS 12/21/2021 BIOSYSTEMS 4dvisory Link Leica Leica 12/21/2021 BIOSYSTEMS 4dvisory Link								
BIOSYSTEMS ECTRA ST Advisory Link Leica HistoCore BIOSYSTEMS FIRIT ST Affected BIOSYSTEMS BIOSYSTEMS BIOSYSTEMS BIOSYSTEMS BIOSYSTEMS BIOSYSTEMS BIOSYSTEMS Advisory Link Leica HistoCore Not Leica BIOSYSTEMS BIOSYSTEMS BIOSYSTEMS BIOSYSTEMS BIOSYSTEMS BIOSYSTEMS ST Advisory Link Leica Leica Leica Leica BIOSYSTEMS Advisory Link Leica Leica BIOSYSTEMS Advisory Link Leica Leica BIOSYSTEMS Advisory Link Leica Leica BIOSYSTEMS BIOSYSTEMS Advisory Link Leica Leica BIOSYSTEMS	Leica HistoCo	ore	Not					12/21/2021
Leica HistoCore Not Leica 12/21/2021 BIOSYSTEMSPIRIT ST Affected BIOSYSTEMS Leica HistoCore Not Leica 12/21/2021 BIOSYSTEMSPRING Affected BIOSYSTEMS ST Advisory Link Leica Leica 12/21/2021 BIOSYSTEMSP300S Affected BIOSYSTEMS Leica Leica 12/21/2021 BIOSYSTEMSV5030 Affected BIOSYSTEMS	BIOSYSTEMSPECT:	'RA	Affected		BIOSYSTEMS			, ,
Affected BIOSYSTEMS BIOSYSTEMS BIOSYSTEMS BIOSYSTEMS Advisory Link Leica HistoCore Not Leica 12/21/2021 BIOSYSTEMS BIOSYSTEMS BIOSYSTEMS BIOSYSTEMS BIOSYSTEMS BIOSYSTEMS ST Advisory Link Leica Leica Not Leica 12/21/2021 BIOSYSTEMS BIOSYSTEMS Advisory Link Leica Leica Not Leica 12/21/2021 BIOSYSTEMS BIOSYSTEMS Advisory Link Leica Leica BIOSYSTEMS BIOSYSTEMS BIOSYSTEMS BIOSYSTEMS Advisory Link Leica Leica 12/21/2021 BIOSYSTEMS BIOSYSTEMS Advisory Link Leica Leica BIOSYSTEMS Advisory Link Leica Leica BIOSYSTEMS BIOSYSTEMS BIOSYSTEMS Advisory Link Leica Leica Not Leica 12/21/2021 BIOSYSTEMS	ST				Advisory Link			
Advisory Link	Leica HistoCo	ore	Not		Leica			12/21/2021
Leica HistoCore Not Leica 12/21/2021 BIOSYSTEM\$PRING ST Leica Leica Leica Not Leica 12/21/2021 BIOSYSTEM\$P300S Affected BIOSYSTEMS Advisory Link Leica Leica Not Leica 12/21/2021 BIOSYSTEM\$P300S Leica Leica Not Leica 12/21/2021 BIOSYSTEM\$V5030 Affected BIOSYSTEMS Advisory Link Leica Leica 12/21/2021 BIOSYSTEM\$V5030 Affected BIOSYSTEMS Advisory Link Leica Leica BIOSYSTEMS BIOSYSTEM\$V5030 Affected BIOSYSTEMS	BIOSYSTEM S IRIT	ST	Affected		BIOSYSTEMS			
BIOSYSTEMS RING ST Advisory Link Leica Leica BIOSYSTEMS Advisory Link Leica Leica BIOSYSTEMS BIOSYSTEMS BIOSYSTEMS Advisory Link Leica Leica Not Leica Leica BIOSYSTEMS Advisory Link Leica Leica BIOSYSTEMS BIOSYSTEMS Advisory Link Leica BIOSYSTEMS Advisory Link Leica BIOSYSTEMS Advisory Link Leica BIOSYSTEMS Advisory Link Leica BIOSYSTEMS BIOSYSTEMS Advisory Link Leica BIOSYSTEMS					Advisory Link			
ST Leica Leica Not Leica 12/21/2021 BIOSYSTEMSP300S Affected BIOSYSTEMS Leica Leica Not Leica 12/21/2021 BIOSYSTEMSV5030 Affected BIOSYSTEMS Advisory Link Leica Leica 12/21/2021 BIOSYSTEMSV5030 Affected BIOSYSTEMS Advisory Link Leica Leica Not Leica 12/21/2021 BIOSYSTEMSSTEMSV5000 Affected BIOSYSTEMS								12/21/2021
Leica Leica Not Leica BIOSYSTEMSP300S Affected BIOSYSTEMS Advisory Link Leica Leica Not Leica 12/21/2021 BIOSYSTEMSV5030 Affected BIOSYSTEMS Advisory Link Leica Leica 12/21/2021 BIOSYSTEMSV5030 Affected BIOSYSTEMS Advisory Link Leica Leica Not Leica 12/21/2021 BIOSYSTEMSV5000 Affected BIOSYSTEMS		G	Affected					
BIOSYSTEMSP300S Affected BIOSYSTEMS Advisory Link Leica Leica BIOSYSTEMS BIOSYSTEMS BIOSYSTEMS BIOSYSTEMS BIOSYSTEMS BIOSYSTEMS Advisory Link Leica Leica Not Leica Leica BIOSYSTEMS Advisory Link Leica Leica BIOSYSTEMS BI								
Advisory Link Leica Leica Not Leica 12/21/2021 BIOSYSTEMS/5030 Affected BIOSYSTEMS Advisory Link Leica Leica Not Leica 12/21/2021 BIOSYSTEMS/4020 Affected BIOSYSTEMS								12/21/2021
Leica Leica Not Leica 12/21/2021 BIOSYSTEMSV5030 Affected BIOSYSTEMS Advisory Link Leica Leica Not Leica 12/21/2021 BIOSYSTEMSY4020 Affected BIOSYSTEMS	BIOSYSTEMSP300	OS	Affected					
BIOSYSTEMSV 5030 Affected BIOSYSTEMS Advisory Link Leica Leica Not Leica 12/21/2021 BIOSYSTEMST 4020 Affected BIOSYSTEMS	T . T .		37 .					10/01/2001
Advisory Link Leica Leica Not Leica 12/21/2021 BIOSYSTEMST4020 Affected BIOSYSTEMS								12/21/2021
Leica Leica Not Leica 12/21/2021 BIOSYSTEMST4020 Affected BIOSYSTEMS	BIOSYSTEMS/5030)	Affected					
BIOSYSTEMS BIOSYSTEMS BIOSYSTEMS	Taina Tain		Net					19/91/9001
								12/21/2021
Advisory Link	D1O3131EM 33 4020		Affected					
					Advisory Link			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Leica	Leica		Not		Leica			12/21/2021
BIOSYST	E N\$S T5010		Affected		BIOSYSTEMS			
					Advisory Link			
Leica	Leica		Not		Leica			12/21/2021
BIOSYST	ENSS 5020		Affected		BIOSYSTEMS			
т •	т •		NT /		Advisory Link			10/01/0001
Leica DIOCVET	Leica EM \$ P1020		Not Affected		Leica BIOSYSTEMS			12/21/2021
DIOSISI	EM13F 1020		Affected		Advisory Link			
Leica	LIS		Under		Leica			12/21/2021
	EMSnnect		Investigat	ion	BIOSYSTEMS			12/21/2021
					Advisory Link			
Leica	PathDX		Not		Leica			12/21/2021
BIOSYST	EMS		Affected		BIOSYSTEMS			, ,
					Advisory Link			
Leica	ThermoBrite	2	Not		Leica			12/21/2021
BIOSYST	EM ES ite		Affected		BIOSYSTEMS			
_					Advisory Link			
Lenovo	BIOS/UEFI		Not		Apache Log4j			2021-12-14
т	CI :		Affected		Vulnerability			0001 10 14
Lenovo	Chassis Manage-		Not Affected		Apache Log4j Vulnerability			2021-12-14
	ment		Affected		vumerability			
	Module 2							
	(CMM)							
Lenovo	Commercial		Not		Apache Log4j			2021-12-14
	Vantage		Affected		Vulnerability			
Lenovo	Confluent		Not		Apache Log4j			2021-12-14
			Affected		Vulnerability			
Lenovo	DSS-G		Affected		Apache Log4j			2021-12-14
					Vulnerability			
Lenovo	Embedded		Not		Apache Log4j			2021-12-14
	System		Affected		Vulnerability			
	Manage-							
	ment							
	Java-based KVM							
	clients							
Lenovo	Fan Power		Not		Apache Log4j			2021-12-14
2011010	Controller		Affected		Vulnerability			2021 12 11
	(FPC)		111100004		, dillordoning			
Lenovo	Fan Power		Not		Apache Log4j			2021-12-14
	Controller2		Affected		Vulnerability			
	(FPC2)							

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Lenovo	Integrated		Not		Apache Log4j			2021-12-14
	Manage-		Affected		Vulnerability			
	ment							
	Module II							
	(IMM2)							
Lenovo	NetApp		Affected		Apache Log4j	See Ne-		2021-12-14
	ONTAP				Vulnerability	tApp		
	Tools for					advisory.	•	
	VMware vSphere							
Lenovo	Network		Not		Apache Log4j			2021-12-14
Lenovo	Switches		Affected		Vulnerability			2021-12-14
	running:		Tinected		vamerability			
	Lenovo							
	CNOS,							
	Lenovo							
	ENOS,							
	IBM							
	ENOS, or							
	Brocade							
т.	FOS		TT 1		A 1 T 4			2021 12 14
Lenovo	Storage		Under	·	Apache Log4j			2021-12-14
	Manage- ment		Investigat	ion	Vulnerability			
	utilities							
Lenovo	System		Not		Apache Log4j			2021-12-14
LCHOVO	Manage-		Affected		Vulnerability			2021-12-14
	ment		Tinected		vamerability			
	Module							
	(SMM)							
Lenovo	System		Not		Apache Log4j			2021-12-14
	Manage-		Affected		Vulnerability			
	ment							
	Module 2							
-	(SMM2)		2.7					
Lenovo	System		Not		Apache Log4j			2021-12-14
т	Update		Affected		Vulnerability			0001 10 14
Lenovo	Thin		Not		Apache Log4j			2021-12-14
	Installer		Affected		Vulnerability			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Lenovo	ThinkAgile HX		Affected		Apache Log4j Vulnerability	Nutanix and VMware components only; hardware not affected. See Nutanix and VMWare		2021-12-14
Lenovo	ThinkAgile VX		Affected		Apache Log4j Vulnerability	advisories. VMware compo- nents only; hard- ware not af- fected. See VMWare advisory.		2021-12-14
Lenovo	ThinkSystem 2x1x16 Digital KVM Switch - Type 1754D1T	1	Not Affected		Apache Log4j Vulnerability	auvisory.		2021-12-14
Lenovo	ThinkSystem DE Series Storage	1	Not Affected		Apache Log4j Vulnerability	See also Ne- tApp advisory.		2021-12-14
Lenovo	ThinkSystem DM Series Storage	1	Not Affected		Apache Log4j Vulnerability	See also Ne- tApp advisory.		2021-12-14
Lenovo	ThinkSystem DS Series Storage	1	Not Affected		Apache Log4j Vulnerability	advibory.		2021-12-14
Lenovo	ThinkSystem Manager (TSM)	1	Not Affected		Apache Log4j Vulnerability			2021-12-14

Vendor	Product Ve	ersion(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Lenovo	Update		Not		Apache Log4j			2021-12-14
	Retriever		Affected		Vulnerability			
Lenovo	Vantage		Not		Apache Log4j			2021-12-14
			Affected		Vulnerability			
Lenovo	XClarity		Affected		Apache Log4j			2021-12-14
	Adminis-				Vulnerability			
	trator							
	(LXCA)							
Lenovo	XClarity		Not		Apache Log4j			2021-12-14
	Controller		Affected		Vulnerability			
	(XCC)							
Lenovo	XClarity		Affected		Apache Log4j			2021-12-14
	Energy				Vulnerability			
	Manager							
	(LXEM)							
Lenovo	XClarity		Not		Apache Log4j			2021-12-14
	Essentials		Affected		Vulnerability			
	(LXCE)				· ·			
Lenovo	XClarity		Under		Apache Log4j			2021-12-14
	Integrator		Investigation	on	Vulnerability			
	(LXCI) for				·			
	Microsoft							
	Azure Log							
	Analytics							
Lenovo	XClarity		Not		Apache Log4j			2021-12-14
	Integrator		Affected		Vulnerability			
	(LXCI) for				3			
	Microsoft							
	System							
	Center							
Lenovo	XClarity		Under		Apache Log4j			2021-12-14
	Integrator		Investigation	on	Vulnerability			
	(LXCI) for		211,000,000	911	, amorasing			
	Nagios							
Lenovo	XClarity		Under		Apache Log4j			2021-12-14
201010	Integrator		Investigation	on	Vulnerability			2021 12 11
	(LXCI) for		111105015001		vallierability			
	ServiceNow							
Lenovo	XClarity		Affected		Apache Log4j			2021-12-14
TOHOVO	Integrator		moud		Vulnerability			2021-12-14
	(LXCI) for				vumerability			
	VMware							
	vCenter							
	v Centrer							

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Lenovo	XClarity Integrator (LXCI) for Windows		Not Affected		Apache Log4j Vulnerability			2021-12-14
	Admin							
Lenovo	Center XClarity		Not		Apache Log4j			2021-12-14
Lenovo	Mobile (LXCM)		Affected		Vulnerability			2021 12 14
Lenovo	XClarity		Not		Apache Log4j			2021-12-14
	Orchestra- tor (LXCO)		Affected		Vulnerability			
Lenovo	XClarity		Not		Apache Log4j			2021-12-14
	Provisioning Manager		Affected		Vulnerability			
LeoStream	(LXPM)				LeoStream			
LCOStream					Discussion			
Let's					Let's Enrypt			
Encrypt					Statement			
LibreNMS					LibreNMS Statement			
LifeRay					LifeRay Blog			
LifeSize					LifeSize			
Lightbend					Statement Lightbend			
O					Statement			
Lime					Lime CRM			
CRM	-				Statement			
LIONGAR	LD				LIONGARD FAQ			
LiquidFiles	5				LiquidFiles			
LiveAction	L				Statement LiveAction Statement			
Loftware					Loftware			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
LOGalyze	SIEM & log analyzer tool	v4.x	Affected	No	abandoned open-source software repo (sourceforge.net)	1.2.17.jar	Forks (github.com) /lib/log4j- che/log4j/net/SocketNode.clas	2021-12-17 s):
LogiAnalyt	tics				LogiAnalytics Statement	1.2.17		
LogicMonit	toŁogicMonito Platform	r	Not Affected		Log4j Security Vulnerabilities			
LogMeIn					LogMeIn Statement			
LogRhythn	n				LogRhythm			
Looker	Looker	21.0, 21.6, 21.12, 21.16, 21.18, 21.20	Affected	Yes	Statement Looker Statement			
LucaNet					LucaNet Statement			
Lucee					Lucee Statement			
Lyrasis	Fedora Repository	3.x,4.x,5.x,6.x	Not Affected		Fedora Repository Statement	Fedora Repository is unaffiliated with Fedora Linux. Uses logback and explicitly excludes log4j.		2021-12-14

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
MailStore					MailStore			
					Statement			
Maltego					Maltego			
					Response to			
					Logj4			
ManageEi	ngi Se rvicedesk	11305 and below	Affected		Manage Engine			12/15/2021
	Plus				Advisory			, ,
ManageEi	ngine				Manage Engine			
Zoho	O .				Link			
ManageEı	ngi A DManager	On-Prem			ManageEngine			12/16/2021
Zoho	Plus				Vulnerability			, ,
					Impact			
ManageEı	ngi A eDAudit	On-Prem			ManageEngine			12/16/2021
Zoho	Plus				Vulnerability			, ,
					Impact			
ManageEi	ngi Data Security	On-Prem			ManageEngine			12/16/2021
Zoho	Plus	0			Vulnerability			//
20110	1 140				Impact			
ManageEi	ngi F eventLog	On-Prem			ManageEngine			12/16/2021
Zoho	Analyzer	On 1 rom			Vulnerability			12/10/2021
20110	Tillely Zer				Impact			
ManageEı	ngi M 365	On-Prem			ManageEngine			12/16/2021
Zoho	Manager	On 1 rom			Vulnerability			12/10/2021
Zono	Plus				Impact			
ManageFi	ngi R ecoveryMan	after Prom			ManageEngine			12/16/2021
Zoho	Plus	agai i iciii			Vulnerability			12/10/2021
20110	Tius				Impact			
ManagoFi	ngi F exchange	On-Prem			ManageEngine			12/16/2021
Zoho	Reporter	On-1 Tem			Vulnerability			12/10/2021
ZOHO	Plus				Impact			
ManagaFi	nginLeog360	On-Prem			ManageEngine			12/16/2021
Zoho	igimeg900	On-1 Tem			Vulnerability			12/10/2021
20110					Impact			
ManagaFi	ngi h æg360	On-Prem			ManageEngine			12/16/2021
ManageEi Zoho	UEBA	Oll-1 Telli			Vulnerability			12/10/2021
20110	UEDA							
ManageEı	ari Claud	On-Prem			Impact ManageEngine			12/16/2021
_	~	On-Frein			Vulnerability			12/10/2021
Zoho	Security				v			
M	Plus	O D			Impact			10/16/0001
ManageE1		On-Prem			ManageEngine			12/16/2021
Zoho	Security				Vulnerability			
М Б	Plus	O D-			Impact			10/10/0001
_	ngi A enalytics	On-Prem			ManageEngine			12/16/2021
Zoho	Plus				Vulnerability			
					Impact			
MariaDB					MariaDB			
					Statement			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
MathWorl	ks All Math- Works general release desktop or server products		Not Affected	No	MathWorks statement regarding CVE-2021-44228			
MathWorl					MathWorks			
Matlab					Matlab			
Matillion					Statement Matillion Security Advisory			
Matomo					Matomo Statement			
Mattermo FocalBoar					Mattermost FocalBoard Concern			
McAfee	Data Exchange Layer (DXL) Client		Not Affected		Concern			12/20/2021
McAfee	Data Loss Prevention (DLP) Discover		Not Affected					12/20/2021
McAfee	Data Loss Prevention (DLP) Endpoint for Mac		Not Affected					12/20/2021
McAfee	Data Loss Prevention (DLP) Endpoint for Windows		Not Affected					12/20/2021
McAfee	Data Loss Prevention (DLP) Monitor		Not Affected					12/20/2021
McAfee	Data Loss Prevention (DLP) Prevent		Not Affected					12/20/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
McAfee	Endpoint Security (ENS) for Linux		Not Affected					12/20/2021
McAfee	Endpoint Security (ENS) for Mac		Not Affected					12/20/2021
McAfee	Endpoint Security (ENS) for Windows		Not Affected					12/20/2021
McAfee	ePolicy Or- chestrator Applica- tion Server	5.10 CU11	Fixed	Yes	https: //kc.mcafee.com/ agent/index? page=content&	,		12/20/2021
McAfee	(ePO) ePolicy Or- chestrator Agent Handlers (ePO-AH)		Not Affected		id=SB10377			12/20/2021
McAfee	Host Intrusion Prevention (Host IPS)		Not Affected					12/20/2021
McAfee	Management of Native Encryption (MNE)		Not Affected					12/20/2021
McAfee	McAfee Active Response (MAR)		Not Affected					12/20/2021
McAfee	McAfee Agent (MA)		Not Affected					12/20/2021
McAfee	McAfee Application and Change Control (MACC) for Linux		Not Affected					12/20/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
McAfee	McAfee Application and Change Control (MACC) for		Not Affected					12/20/2021
McAfee	Windows McAfee Client Proxy (MCP) for Mac		Not Affected					12/20/2021
McAfee	McAfee Client Proxy (MCP) for Windows		Not Affected					12/20/2021
McAfee	McAfee Drive Encryption (MDE)		Not Affected					12/20/2021
McAfee	McAfee Security for Microsoft Exchange (MSME)		Not Affected					12/20/2021
McAfee	McAfee Security for Microsoft SharePoint (MSMS)		Not Affected					12/20/2021
McAfee	McAfee Security for Microsoft Exchange (MSME)		Not Affected					12/20/2021
McAfee	Enterprise Security Manager (ESM)	11.5.3	Fixed	Yes	https: //kc.mcafee.com/ agent/index? page=content& id=SB10377			12/20/2021
McAfee	Network Security Manager (NSM)		Not Affected		M-0010011			12/20/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
McAfee	Network Security Platform (NSP)		Not Affected					12/20/2021
McAfee	Policy Auditor		Not Affected					12/20/2021
McAfee	Threat Intelligence Exchange (TIE)		Affected		https: //kc.mcafee.com/ agent/index? page=content& id=SB10377	Latest status in linked Secu- rity Bulletin		12/20/2021
McAfee	Web Gateway (MWG)		Foxed		https: //kc.mcafee.com/ agent/index? page=content& id=SB10377	2 4.1.001.1		12/20/2021
Medtronic MEINBER	a.G		Under Investigati	on	Medtronic Advisory Link MEINBERG			12/21/2021
1,1211,1211,					Information			
Meltano	Meltano		Not affected		Meltano	Project is written in Python		
Memurai MicroFocu	s				Memurai Information MicroFocus	·		
Microsoft	Azure Application Gateway		Not Affected		Statement Microsoft's Response to CVE-2021-44228 Apache Log4j 2			
Microsoft	Azure API Gateway		Not Affected		Microsoft's Response to CVE-2021-44228 Apache Log4j 2			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated	
Microsoft	Azure Data lake store java	< 2.3.10	Affected		azure-data-lake- store- java/CHANGES.	md			
					at	0.0000 4.1	4FF 000 00 140		
					ed5d6304783286c	3cfff0a1dee	457a922e23ad48		
					· Azure/azure- data-lake-store-				
					java ·				
					GitHub				
Microsoft	Azure Data	< 2.3.10	Affected		azure-data-lake-				
	lake store				store-				
	java				java/CHANGES.	md			
					at				
					ed5d6304783286c	3cfff0a1dee	457a922e23ad48		
					· Azure/azure-				
					data-lake-store- java ·				
					GitHub				
Microsoft	Azure	2019.0 - 2020.1	Affected	No	Azure DevOps				
	DevOps				(and Azure				
	Server				DevOps Server)				
					and the log4j				
					vulnerability				
Microsoft	Azure		Not		Azure DevOps				
	DevOps)ps	Affected	Affected		(and Azure			
					DevOps Server)				
					and the log4j vulnerability				
Microsoft	Azure		Not		Microsoft's				
	Traffic		Affected		Response to				
	Manager				CVE-2021-44228				
					Apache Log4j 2				
Microsoft	Team	2018.2+	Affected	No	Azure DevOps				
	Foundation				(and Azure				
	Server				DevOps Server)				
					and the log4j vulnerability				
Microstrate	eov				Microstrategy				
1,1101000100	~8 <i>J</i>				Statement				
Midori					Midori Global				
Global					Statement				
Mikrotik					Mikrotik				
					Statement				
Milestone					Milestone sys				
Sys Mimograf					Statement				
Mimecast					Mimecast				
					Information				

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Minecraft					Minecraft			
					Vulnerability			
					Message			
Mirantis					Mirantis			
					Statement			
Miro					Miro Log4j			
					Updates			
Mitel					Mitel Statement			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
MobileIron		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	12/20/21
						portal during the pro- cedure, how- ever, end user	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
MobileIron		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	12/20/21
						admin portal during the pro- cedure, how- ever, end user	

MobileIron	D						
	Reporting Database (RDB)	All Versions	Affected	Yes	https://forums. ivanti.com/s/ article/Security- Bulletin-CVE- 2021-44228- Remote-code- injection-in- Log4j?language= en_US	The mitigation instructions listed in a subsequent section removes a vulnerable Java class (JNDILookUp.class) from the affected Log4J Java library and as a result removes the ability to perform the RCE attack. The workaround needs to be applied in a maintenance window. You will not be able to access the	12/20/21
					339	admin portal during the pro- cedure, how- ever, end user	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
MobileIron	Sentry	9.13, 9.14	Affected	Yes	https://forums. ivanti.com/s/ article/Security- Bulletin-CVE- 2021-44228- Remote-code- injection-in- Log4j?language= en_US	The mitigation instructions listed in a subsequent section removes a vulnerable Java class (JNDILookUp.class) from the affected Log4J Java library and as a result removes the ability to perform the RCE attack. The workaround needs to be applied in a maintenance window. You will not	12/20/21
					340	be able to access the admin portal during the pro- cedure, how- ever, end user	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
MongoDB	All other components of MongoDB Atlas (including Atlas Database, Data Lake, Charts)		Not Affected		https: //www.mongodb. com/blog/post/ log4shell- vulnerability-cve- 2021-44228-and- mongodb			
MongoDB	MongoDB Atlas Search		Affected	yes	https: //www.mongodb. com/blog/post/ log4shell- vulnerability-cve- 2021-44228-and- mongodb			
MongoDB	MongoDB Community Edition (including Community Server, Cloud Manager, Community Kubernetes Operators)		Not Affected		https: //www.mongodb. com/blog/post/ log4shell- vulnerability-cve- 2021-44228-and- mongodb			
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			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
MongoDB	MongoDB		Not		https:			
	Realm		Affected		//www.mongodb.			
	(including				com/blog/post/			
	Realm				log4shell-			
	Database,				vulnerability-cve-			
	Sync,				2021-44228-and-			
	Functions,				mongodb			
	APIs)							
MongoDB	MongoDB		Not		https:			
MongoDD	Tools		Affected		//www.mongodb.			
	(including		Tinected		com/blog/post/			
	Compass,				log4shell-			
	Database				vulnerability-cve-			
	Shell, VS				2021-44228-and-			
	Code							
					mongodb			
	Plugin,							
	Atlas CLI,							
	Database							
N. 11	Connectors)				3.6 11			
Moodle					Moodle			
3.F. C. C.					Discussion			
MoogSoft					MoogSoft			
					Vulnerability			
					Information			
Motorola					Motorola			
Avigilon					Avigilon			
					Technical			
					Notification			
Mulesoft					Mulesoft	This		
					Statement	advi-		
						sory is		
						avail-		
						able to		
						cus-		
						tomers		
						only		
						and has		
						not		
						been re-		
						viewed		
						by CISA		
						01011		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Mulesoft	Mule Runtime	3.x,4.x	Affected	Yes	Apache Log4j2 vulnerability - December 2021	This advisory is available to account holders only and has not been reviewed by		12/15/2021
Mulesoft	Mule Agent	6.x	Affected	Yes	Apache Log4j2 vulnerability - December 2021	CISA. This advisory is available to account holders only and has not been reviewed by		12/15/2021
Mulesoft	Cloudhub		Affected	Yes	Apache Log4j2 vulnerability - December 2021	CISA. This advisory is available to account holders only and has not been re- viewed by CISA.		12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Mulesoft	Anypoint Studio	7.x	Affected	Yes	Apache Log4j2 vulnerability - December 2021	This advisory is available to account holders only and has not been reviewed by CISA.		12/15/2021
N-able Nagios NAKIVO					N-able Statement Nagios Statement NAKIVO	OISA.		
NAKIVO					Statement			
Neo4j	Neo4j Graph Database	Version >4.2, <42.12	Affected	No				12/13/2021
Netapp	Multiple NetApp products		Affected		https://security. netapp.com/ advisory/ntap- 20211210-0007/			
NetCup NetGate PFSense					Netcup Statement NetGate PFSense Forum			
Netwrix					Netwrix Statement			
New Relic	Containerize Private Minion (CPM)	ed 3.0.57	Fixed	Yes	NR21-04	New Relic is in the process of revis- ing guid- ance/doc how- ever the fix version re- mains	Security Bulletin NR21-04 cumentation,	12-18-2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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/ NextCloud Help	Initially fixed in 7.4.2, but ad- ditional vulner- ability found	New Relic tracking, covers CVE-2021-44228, CVE-2021-45046	12/20/2021
Nextflow Nexus	Nextflow	21.04.0.5552	Not Affected		https: //www.nextflow. io/docs/latest/ index.html Nexus Group			12/21/2021
Group NI (National Instrument	ss)				Docs NI Support Link			
Nice Software (AWS) EnginFRA	ME				Nice Software EnginFRAME Link			
NinjaRMM	[NinjaRMM Article	This advisory is available to		
						tomers only and has not been re-		
						viewed by CISA		
Nomachine NoviFlow Nulab Nulab	Backlog Backlog	N/A (SaaS) < 1.11.7	Fixed Fixed	Yes	Nomachine Forums Noviflow Link Nulab Blog Post Nulab Blog Post			
	Enterprise (On- premises)			100				
Nulab	Cacoo	N/A (SaaS)	Fixed		Nulab Blog Post			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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 Advisory			12/20/2021
Nutanix	AOS	LTS (including Prism Element), Community Edition	Not Affected		Nutanix Security Advisory			12/20/2021
Nutanix	AOS	STS (including Prism Element)	Fixed	Yes	Nutanix Security Advisory	Patched in 6.0.2.4, available on the Portal for		
download Nutanix	Beam	12/20/2021	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	Tidvisory.		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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Nutanix	Era	All	Not		Nutanix Security			12/20/2021
Nutanix	File Analytics	2.1.x, 2.2.x, 3.0+	Affected Affected		Advisory Nutanix Security Advisory Advisory	Mitigated in version 3.0.1 which is available on the Portal for download. Mitigation is	1	12/20/2021 12/20/2021
						avail- able here		
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	114,1501		12/20/2021
Nutanix	Frame		Fixed		Nutanix Security Advisory	Saas- Based Procuct. See Advisory.		12/20/2021
Nutanix	FrameGov		Fixed		Nutanix Security Advisory			12/20/2021
Nutanix	FSCVM	All	Not Affected		Nutanix Security Advisory	v		12/20/2021
Nutanix	Insights		Not Affected		Nutanix Security Advisory	Saas- Based Procuct. See Advisory.		12/20/2021

Vendor	Product	Version(s)	Status Update Available	Vendor Link	Notes Other References	Last Updated
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	ridvisory.	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 avail- able 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
Nutanix	Objects	All	Affected	Nutanix Security Advisory	Mitigation is avail-able here	12/20/2021
Nutanix	Prism Central	All	Fixed	Nutanix Security Advisory	Patched in 2021- 9.0.3, avail- able on the Portal for download.	12/20/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Nutanix	Sizer		Fixed		Nutanix Security Advisory	Saas- Based Procuct. See		12/20/2021
Nutanix	Volumes	All	Not Affected		Nutanix Security Advisory	Advisory.		12/20/2021
Nutanix	Witness VM	All	Affected		Nutanix Security Advisory	Mitigatio is avail- able here	on	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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Okta	Okta		Not		Okta's response			12/12/2021
	LDAP		Affected		to			
	Agent				CVE-2021-44228			
					("Log4Shell")			
					Okta Security			
Okta	Okta		Not		Okta's response			12/12/2021
	Mobile		Affected		to			
					CVE-2021-44228			
					("Log4Shell")			
					Okta Security			
Okta	Okta	< 2.17.0	Affected		Okta RADIUS			12/12/2021
	RADIUS				Server Agent			, ,
	Server				CVE-2021-44228			
	Agent				Okta			
Okta	Okta Verify		Not		Okta's response			12/12/2021
			Affected		to			
					CVE-2021-44228			
					("Log4Shell")			
					Okta Security			
Okta	Okta		Not		Okta's response			12/12/2021
	Workflows		Affected		to			
					CVE-2021-44228			
					("Log4Shell")			
					Okta Security			
Okta	Okta	< 1.4.6	Affected		Okta On-Prem			12/12/2021
	On-Prem				MFA Agent			
	MFA Agent				CVE-2021-44228			
					Okta			
Onespan					Onespan Link			
Opengear					Opengear Link			
OpenMRS					OpenMRS TALK			
TALK					Link			
OpenNMS					OpenNMS Link			
OpenSearc	:h				OpenSearch			
					Discussion Link			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Oracle			Affected		Oracle Security Alert My Oracle Support Document	The support document is available to customers only and has not been reviewed by CISA		12/17/2021
Orgavision	1				Orgavision Link	CISA		
Osirium	PAM		Not		Osirium			
			Affected		statement			
Osirium	PEM		Not		Osirium			
0	DD4		Affected		statement			
Osirium	PPA		Not Affected		Osirium statement			
OTRS OVHCloud	d		Affected		OTRS Link OVHCloud Blog Post			
OwnCloud	l				OwnCloud Link			
OxygenXN			Affected	Fixed	Yes	https:		12/17/2021
						//www. oxygenxn com/ security/ advisory/ CVE- 2021- 44228. html		
OxygenXN	MLDeveloper		Affected	Fixed	Yes	https: //www. oxygenxn com/ security/ advisory/ CVE- 2021- 44228. html		12/17/2021

Vendor Produc	et Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
OxygenXMLEditor		Affected	Fixed	Yes	https: //www. oxygenxml. com/ security/ advisory/ CVE- 2021- 44228. html	12/17/2021
OxygenXMLOxyger Conten Fusion		Affected	Fixed	Yes	https: //www. oxygenxml. com/ security/ advisory/ CVE- 2021- 44228. html	12/17/2021
OxygenXMLOxyger Feedba Enterp	ck	Affected	Fixed	Yes	https: //www. oxygenxml. com/ security/ advisory/ CVE- 2021- 44228. html	12/17/2021
OxygenXMLOxyger License Server		Affected	Fixed	Yes	https: //www. oxygenxml. com/ security/ advisory/ CVE- 2021- 44228. html	12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Update
OxygenXM	MLOxygen PDF Chemistry	v22.1, 23.0, 23.1, 24.0	Affected	Fixed	Yes	https: //www. oxygenxml. com/ security/ advisory/ CVE- 2021- 44228. html	12/17/2021
OxygenXM	MLOxygen SDK		Affected	Fixed	Yes	https: //www. oxygenxml. com/ security/ advisory/ CVE- 2021- 44228. html	12/17/2021
OxygenXM	MLPlugins (see advisory link)		Affected	Fixed	Yes	https: //www. oxygenxml. com/ security/ advisory/ CVE- 2021- 44228. html	12/17/2021
OxygenXN	MLPublishing Engine		Affected	Fixed	Yes	https: //www. oxygenxml. com/ security/ advisory/ CVE- 2021- 44228. html	12/17/2021

Vendor F	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
OxygenXMLV	Web Author		Affected	Fixed	Yes	https: //www. oxygenxml. com/ security/ advisory/ CVE- 2021- 44228. html	12/17/2021
OxygenXMLV	WebHelp		Affected	Fixed	Yes	https: //www. oxygenxml. com/ security/ advisory/ CVE- 2021- 44228. html	12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Palantir	Palantir	All	Fixed		Palantir	No	12/19/2021
	Foundry				Response to	impact	
					Log4j	to	
					Vulnerability	Palantir-	
					(palantir.com)	hosted	
					,	or	
						Apollo-	
						connected	
						in-	
						stances,	
						and up-	
						dates	
						have	
						been	
						de-	
						ployed	
						for full	
						remedi-	
						ation.	
						Discon-	
						nected	
						cus-	
						tomer	
						in-	
						stances	
						may	
						require	
						manual	
						updates.	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Palantir	Palantir Gotham	All	Fixed		Palantir Response to Log4j Vulnerability (palantir.com)	No impact to Palantir- hosted or Apollo- connected in- stances, and up- dates have been de- ployed for full remedi- ation. Discon- nected cus- tomer in- stances may	12/19/2021
Palantir	Palantir Apollo	All	Not Affected		Palantir Response to Log4j Vulnerability (palantir.com)	require manual updates. No impact, and updates have been de- ployed for full remediation.	12/19/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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 (paloaltonet- works.com)	upuaics.		
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 (paloaltonet- works.com)			
Palo-Alto Networks	Cortex Data Lake		Not Affected		CVE-2021-44228 Informational: Impact of Log4j Vulnerability CVE-2021-44228 (paloaltonet- works.com)			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Palo-Alto	Cortex		Not		CVE-2021-44228			
Networks	Xpanse		Affected		Informational:			
					Impact of Log4j			
					Vulnerability			
					CVE-2021-44228			
					(paloaltonet-			
					works.com)			
Palo-Alto	Cortex		Not		CVE-2021-44228			
Networks	XDR		Affected		Informational:			
	Agent				Impact of Log4j			
					Vulnerability			
					CVE-2021-44228			
					(paloaltonet-			
					works.com)			
Palo-Alto	Cortex		Not		CVE-2021-44228			
Networks	XSOAR		Affected		Informational:			
					Impact of Log4j			
					Vulnerability			
					CVE-2021-44228			
					(paloaltonet-			
					works.com)			
Palo-Alto	Expedition		Not		CVE-2021-44228			
Networks			Affected		Informational:			
					Impact of Log4j			
					Vulnerability			
					CVE-2021-44228			
					(paloaltonet-			
					works.com)			
Palo-Alto	IoT		Not		CVE-2021-44228			
Networks	Security		Affected		Informational:			
					Impact of Log4j			
					Vulnerability			
					CVE-2021-44228			
					(paloaltonet-			
					works.com)			
	GlobalProte	ect	Not		CVE-2021-44228			
Networks	App		Affected		Informational:			
					Impact of Log4j			
					Vulnerability			
					CVE-2021-44228			
					(paloaltonet-			
					works.com)			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Palo-Alto	Palo-Alto		Not		CVE-2021-44228			
Networks	Networks-		Affected		Informational:			
	OS for				Impact of Log4j			
	Firewall				Vulnerability			
	and				CVE-2021-44228			
	Wildfire				(paloaltonet-			
					works.com)			
Palo-Alto	Prisma		Not		CVE-2021-44228			
Networks	Access		Affected		Informational:			
					Impact of Log4j			
					Vulnerability			
					CVE-2021-44228			
					(paloaltonet-			
					works.com)			
Palo-Alto	Prisma		Not		CVE-2021-44228			
Networks	Cloud		Affected		Informational:			
					Impact of Log4j			
					Vulnerability			
					CVE-2021-44228			
					(paloaltonet-			
					works.com)			
Palo-Alto	Prisma		Not		CVE-2021-44228			
Networks	Cloud		Affected		Informational:			
	Compute				Impact of Log4j			
					Vulnerability			
					CVE-2021-44228			
					(paloaltonet-			
					works.com)			
Palo-Alto	Okyo		Not		CVE-2021-44228			
Networks	Grade		Affected		Informational:			
					Impact of Log4j			
					Vulnerability			
					CVE-2021-44228			
					(paloaltonet-			
					works.com)			
Palo-Alto			Not		CVE-2021-44228			
Networks	Security		Affected		Informational:			
					Impact of Log4j			
					Vulnerability			
					CVE-2021-44228			
					(paloaltonet-			
					works.com)			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Palo-Alto	WildFire		Not		CVE-2021-44228			
Networks	Appliance		Affected		Informational:			
					Impact of Log4j			
					Vulnerability			
					CVE-2021-44228			
					(paloaltonet-			
					works.com)			
Palo-Alto	WildFire		Not		CVE-2021-44228			
Networks	Cloud		Affected		Informational:			
					Impact of Log4j			
					Vulnerability			
					CVE-2021-44228			
					(paloaltonet-			
					works.com)			
Palo-Alto	User-ID		Not		CVE-2021-44228			
Networks	Agent		Affected		Informational:			
					Impact of Log4j			
					Vulnerability			
					CVE-2021-44228			
					(paloaltonet-			
					works.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 avail- able in reference. Upgrade to PaperCut NG/MF version 21.2.3 Now Avail- able to	12/16/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
PaperCut		21.0 and later	Affected	Yes	https://www.papercut.com/support/known-issues/?id=PO-684#ng	Versions 21.0 and later are im- pacted. Ver- sions 20 and earlier are NOT im- pacted by this. Workaround manual steps avail- able in refer- ence. Up- grade to Pa- perCut NG/MF version 21.2.3 Now Avail-	12/16/2021
Parallels Parse.ly					Parellels Link Parse.ly Blog Post	able to resolve.	

Vendor	Product	Version(s)	Status Update Available	Vendor Link	Notes Oth	er References	Last Updated
PBXMoni	torRMM for 3CX PBX		Not Affected	PBXMonitor Changelog	Mirror Servers were also checked to ensure Log4J was not in- stalled or being used by any of our		12/22/2021
Pega Pentaho				Pega Docs Link Pentaho Support Link	systems.		
Pepperl+l Percona Pexip Phenix Id Philips	Fuchs Multiple		Under Investigation	Pepperl+Fuchs Advisory Link Percona Blog Post Pexip Link Phenix Id Support Link Philips Security			12/21/2021
PHOENIX	products C Physical T products containing firmware		Not Affected	Advisory PHOENIX CONTACT Advisory Link			12/22/2021
	X Software T Products		Not Affected	PHOENIX CONTACT Advisory Link			12/22/2021
PHOENIX CONTAC	Cloud T Services		Affected	PHOENIX CONTACT Advisory Link	Partly af- fected. Reme- dia- tions are being implemented.		12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Ping Identity	PingAccess	4.0 <= version <= 6.3.2	Affected	Yes	Log4j2 vulnerability CVE-2021-44228			2021-12-15
Ping Identity	PingCentral		Affected	Yes	Log4j2 vulnerability CVE-2021-44228			2021-12-15
Ping Identity	PingFederate	8.0 <= version <= 10.3.4	Affected	Yes	Log4j2 vulnerability CVE-2021-44228			2021-12-15
Ping Identity	PingFederate Java Integration Kit	< 2.7.2	Affected	Yes	Log4j2 vulnerability CVE-2021-44228			2021-12-15
Ping Identity	PingFederate OAuth Playground	< 4.3.1	Affected	Yes	Log4j2 vulnerability CVE-2021-44228			2021-12-15
Ping Identity	PingIntelliger	nce	Affected	Yes	Log4j2 vulnerability CVE-2021-44228			2021-12-15
Pitney Bowes Planmeca					Pitney Bowes Support Link Planmeca Link			
Planon Software					Planon News	This advi-		
						sory is avail-		
						able for cus-		
						tomers only and has		
						not been re-		
						viewed by		
Platform.S	Н				Platform.SH	CISA		
Plesk					Blog Post Plesk Support Link			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Plex	Plex Industrial IoT		Fixed		PN1579 - Log4Shell Vulnerability Notice	The product has been updated to Log4j version 2.15. An additional patch is being developed to update to 2.16. No user interaction is		12/15/2021
Polycom					Polycom Support	required.		
Portainer					Link Portainer Blog			
PortSwigg	ger				Post PortSwigger			
PostGreS	QL				$\begin{array}{c} {\rm Forum} \\ {\rm PostGreSQL} \end{array}$			
Postman					News Postman Support			
Power Admin LLC	PA File Sight	NONE	Not Affected		Link Update December 2021: None of our products (PA Server Monitor, PA Storage Monitor, PA File Sight and PA WatchDISK), and none of our websites, use log4j. One less thing to worry about			12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Power Admin LLC	PA Storage Monitor	NONE	Not Affected		Update December 2021: None of our products (PA Server Monitor, PA Storage Monitor, PA File Sight and PA WatchDISK), and none of our websites, use log4j. One less thing to worry			12/17/2021
Power Admin LLC	PA Server Monitor	NONE	Not Affected		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 worry			12/17/2021
Pretix PrimeKey					about Pretix Blog Post PrimeKey			
Progress / IpSwitch					Support Link Progress / IpSwitch Link			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
ProofPoint		· CLOSON(B)	Secution	C petavo Transion	ProofPoint Article	This advisory is available for customers only and has not been reviewed		Eur Optawed
ProSeS Prosys Proxmox PRTG					ProSeS Link Prosys News Link Proxmox Forum PRTG Paessler	by CISA		
Paessler PTC	Axeda Platform	6.9.2	Affected	No	Link 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 PTV	ThingsWorx Analytics	8.5,9.0,9.1,9.2, All supported versions	Affected	No	ThingWorx Apache log4j vulnerability - Incident Response PTV Group Link			12/17/2021
Group Pulse Secure	Ivanti Connect Secure (ICS)		Not Affected		Pulse Secure Article: KB44933 - CVE-2021-44228 - Java logging library (log4j)			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Pulse Secure	Ivanti Neurons for secure		Not Affected		Pulse Secure Article: KB44933			
	Access				CVE-2021-44228 - Java logging library (log4j)			
Pulse	Ivanti		Not		Pulse Secure			
Secure	Neurons for ZTA		Affected		Article: KB44933			
					CVE-2021-44228 - Java logging library (log4j)			
Pulse	Pulse		Not		Pulse Secure			
Secure	Connect Secure		Affected		Article: KB44933			
					CVE-2021-44228 - Java logging			
D .	.				library (log4j)			
Pulse Secure	Pulse Desktop		Not Affected		Pulse Secure Article: KB44933			
	Client				- CVE-2021-44228			
					- Java logging			
Pulse	Pulse		Not		library (log4j) Pulse Secure			
Secure	Mobile Client		Affected		Article: KB44933			
	0.22.22.0				CVE-2021-44228			
					- Java logging library (log4j)			
Pulse	Pulse One		Not		Pulse Secure			
Secure			Affected		Article: KB44933			
					CVE-2021-44228			
					- Java logging library (log4j)			
Pulse	Pulse		Not		Pulse Secure			
Secure	Policy Secure		Affected		Article: KB44933			
	Socaro				CVE-2021-44228			
					- Java logging library (log4j)			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Pulse Secure	Pulse Secure Services Director		Not Affected		Pulse Secure Article: KB44933 - CVE-2021-44228 - Java logging library (log4j)			
Pulse Secure	Pulse Secure Virtual Traffic Manager		Not Affected		Pulse Secure Article: KB44933 - CVE-2021-44228 - Java logging library (log4j)			
Pulse Secure	Pulse Secure Web Applica- tion 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			
Puppet					library (log4j) Puppet Blog Post	mı ·		
Pure Storage			N.		Pure Storage Support Link	This advisory is available for customers only and has not been reviewed by CISA		
Pulse Secure	Ivanti Neurons for ZTA		Not Affected		Pulse Secure Article: KB44933 - CVE-2021-44228 - Java logging library (log4j)			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other Refe	erences	Last Updated
Pulse Secure	Ivanti Neurons for secure		Not Affected		Pulse Secure Article: KB44933			
	Access				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 ex-	1	12/15/2021
Pure	Flash	5.3.x, 6.0.x, 6.1.x,	Affected	No	Pure Storage	pected 12/24/2021 Patch		12/15/2021
Storage	Array	6.2.x			Customer Portal	ex- pected 12/20/2021		
Pure Storage	Cloud Blockstore	CBS6.1.x, CBS6.2.x	Affected	No	Pure Storage Customer Portal	Patch ex- pected	1	12/15/2021
Pure Storage	Pure1	N/A	Fixed	Yes	Pure Storage Customer Portal	12/27/2021]	12/15/2021
Pure Storage Pyramid Analytics	PortWorx	2.8.0+	Affected	Yes	Pure Storage Customer Portal Pyramid Analytics Community Link		1	12/15/2021
QF-Test					QF-Test Blog Post			
Qlik					Qlik Community Link			
QMATIC	Orchestra Central	6.0+	Not Affected		QMATIC Link		1	12/21/2021
QMATIC	Appointment Booking	2.4+	Affected	Yes	QMATIC Link	Update to v. 2.8.2 which con-	1	12/21/2021
QMATIC	Insights	Cloud	Affected	Yes	QMATIC Link	tains log4j 2.16 log4j 2.16	į	12/21/2021
						applied 2021- 12-16		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
QMATIC	Appointment Booking	Cloud/Managed Service	Affected	Yes	QMATIC Link	log4j 2.16 applied 2021- 12-15		12/21/2021
QNAP			Under Investigation	on	QNAP Security Advisory			
QOPPA QSC Q-SYS QT			Not	511	QOPPA Link QSC Q-SYS Article QT			
Q1			Affected		Q I			
Quest Global					Quest Global			
R R2ediviewe	R	4.1.1	Not Affected		https://www.r- project.org/ R2ediviewer Link			12/21/2021
Radware	31				Radware Support Link			
Rapid7	AlcidekArt, kAdvisor, and kAudit	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	AppSpider Enterprise	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	AppSpider Pro	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	Insight Agent	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	InsightAppSe Scan Engine	con-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	InsightAppSe Scan Engine	con-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	0	Seen/-Pireny Cloud	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	InsightConne Orchestrator	cton-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	InsightIDR Network Sensor	on-prem	Not Affected		Rapid7 Statement			12/15/2021
Rapid7	InsightIDR/In Collector & Event Sources	nsigłpt∂ps	Not Affected		Rapid7 Statement			12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Rapid7	InsightOps DataHub	InsightOps DataHub <= 2.0	Affected	Yes	Rapid7 Statement	Upgrade DataHub to version 2.0.1 using the fol- lowing instruc- tions.	12/15/2021
Rapid7	InsightOps non-Java logging libraries	on-prem	Not Affected		Rapid7 Statement		12/15/2021
Rapid7	InsightOps r7insight_jar logging library	<=3.0.8	Affected	Yes	Rapid7 Statement	Upgrade r7insight_java to 3.0.9	12/15/2021
Rapid7	InsightVM Kubernetes Monitor	on-prem	Not Affected		Rapid7 Statement		12/15/2021
Rapid7	InsightVM/N	Ne wpopre m	Not Affected		Rapid7 Statement		12/15/2021
Rapid7	InsightVM/I Console	Ле мрерм ет	Not Affected		Rapid7 Statement	Installations of the InsightVM/Nexpose have "log4j- over- slf4j- 1.7.7.jar" pack- aged in them. This is a differ- ent library than log4j- core and is not vul- nerable to Log4Shell.	12/15/2021

Vendor	Product	Version(s)	Status Update Available	Vendor Link	Notes Other References	Last Updated
Rapid7	InsightVM/	/Ne spese em	Not	Rapid7	Installations	12/15/2021
•	Engine		Affected	Statement	of the	, ,
	O				In-	
					sightVM/Nexpose	
					have	
					" $\log 4$ j-	
					over-	
					slf4j-	
					1.7.7.jar"	
					pack-	
					aged in	
					them.	
					This is	
					a differ-	
					ent	
					library	
					than	
					log4j-	
					core	
					and is	
					not vul-	
					nerable	
					to	
					Log4Shell.	
Rapid7	IntSights	on-prem	Not	Rapid7		12/15/2021
	virtual appliance		Affected	Statement		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Rapid7	Logentries	Linux version	Affected	Yes	Rapid7	Linux:		12/15/2021
-	DataHub	<= 1.2.0.820;			Statement	Install		, ,
		Windows version					b_1.2.0.822.deb	
		<= 1.2.0.820				using		
		112101020				the fol-		
						lowing		
						instruc-		
						tions.		
						Win-		
						dows:		
						Run		
						version		
						1.2.0.822	2	
						in a		
						Docker		
						con-		
						tainer		
						or as a		
						Java		
						com-		
						mand		
						per		
						these		
						instruc-		
						tions.		
						You		
						can		
						find		
						more		
						details		
						here.		
Rapid7	Logentries	All versions: this	Affected	Yes	Rapid7	Migrate		12/15/2021
•	le_java	is a deprecated			Statement	to		, ,
	logging	component				version		
	library	-				$3.0.9 ext{ of}$		
	v					r7insight	_java	
Rapid7	Metasploit	on-prem	Not		Rapid7	O		12/15/2021
•	Framework	•	Affected		Statement			, ,

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 configu- rations applied to it that miti- gate 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	106 J.	12/15/2021
Rapid7 Raritan	Velociraptor	on-prem	Not Affected		Rapid7 Statement Raritan Support Link		12/15/2021
Ravelin Real- Time Innova- tions (RTI)	Distributed Logger		Not Affected		Ravelin Link RTI Statement		12/16/2021
Real- Time Innova- tions (RTI)	Recording Console		Not Affected		RTI Statement		12/16/2021
Real- Time Innova- tions (RTI)	RTI Adminis- tration Console		Not Affected		RTI Statement		12/16/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Real-	RTI Code		Not		RTI Statement		12/16/2021
Time	Generator		Affected				
Innova-							
tions (RTI)							
Real-	RTI Code		Not		RTI Statement		12/16/2021
Time	Generator		Affected				, ,
Innova-	Server						
tions							
(RTI) Real-	RTI Micro	as part of RTI	Affected		RTI Statement		12/16/2021
Time	Applica-	Connext Micro	Anecteu		Tt11 Statement		12/10/2021
Innova-	tion	3.0.0, 3.0.1, 3.0.2,					
tions	Generator	3.0.3					
(RTI)	(MAG)	, C DEDI	A.C 1		DITT CL. 4		10/10/0001
Real- Time	RTI Micro Applica-	as part of RTI Connext	Affected		RTI Statement		12/16/2021
Innova-	tion	Professional 6.0.0					
tions	Generator	and $6.0.1$					
(RTI)	(MAG)						
Real- Time	RTI Monitor		Not Affected		RTI Statement		12/16/2021
Inne Innova-	Monitor		Affected				
tions							
(RTI)							
Red Hat	Red Hat	7	Fixed	Yes	CVE-2021-44228-	Maven	$\mathrm{Dec}/21/2021$
	JBoss Enterprise				Red Hat Customer Portal	Patch - Affects	
	Enterprise Applica-				Customer Fortar	only	
	tion					the	
	Platform					Mav-	
						enized	
						distri- bution.	
						Con-	
						tainer,	
						Zip and	
						RPM	
						distro aren't	
						arent	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Red Hat	Red Hat Process Automation	7	Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	Maven Patch - Affects only the Mav- enized distri- bution. Con- tainer, Zip and RPM distro aren't	Dec/21/2021
						affected.	
Red Hat	Red Hat CodeReady Studio	12.21.0	Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	CRS 12.21.1 Patch	$\mathrm{Dec}/21/2021$
Red 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 Camel K		Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	RHSA- 2021:5130	$\mathrm{Dec}/21/2021$
Red Hat	Red Hat Integration Camel Quarkus		Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	RHSA- 2021:5126	$\mathrm{Dec}/21/2021$
Red Hat	Red Hat JBoss A-MQ Streaming		Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	RHSA- 2021:5138	$\mathrm{Dec}/21/2021$
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 Open- Shift Con- tainer Platform 3.11	openshift3/os logging- elasticsearch		Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	RHSA- 2021:5094	Dec/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Red Hat Open- Shift Con- tainer Platform 4	openshift4/logging-elasticsearch		Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	Please refer to Red Hat Cus- tomer Portal to find the right errata for your		Dec/21/2021
Red Hat Open- Shift Con- tainer Platform 4	openshift4/metering-hive	ose-	Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	version. Please refer to Red Hat Cus- tomer Portal to find the right errata for your		Dec/21/2021
Red Hat Open- Shift Con- tainer Platform 4	openshift4/metering-presto	ose-	Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	version. Please refer to Red Hat Cus- tomer Portal to find the right errata for your version.		Dec/21/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Red Hat Open- Shift Logging	logging- elasticsearch container	6-	Fixed	Yes	CVE-2021-44228- Red Hat Customer Portal	Please refer to Red Hat Cus- tomer Portal to find the right errata for your version.		Dec/21/2021
Red Hat	Red Hat Single Sign-On	7	Not Affected		CVE-2021-44228- Red Hat Customer Portal	version.		$\mathrm{Dec}/21/2021$
Red Hat	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			Dec/21/2021
Red Hat Software Collections	maven35-		Not Affected		CVE-2021-44228- Red Hat Customer Portal			Dec/21/2021
Red Hat Software Collections	rh- maven36- log4j12		Not Affected		CVE-2021-44228- Red Hat Customer Portal			Dec/21/2021
Red Hat	log4j-core		Not Affected		CVE-2021-44228- Red Hat Customer Portal			Dec/21/2021
Red Hat	Satellite 5		Not Affected		CVE-2021-44228- Red Hat Customer Portal			$\mathrm{Dec}/21/2021$

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Red Hat	Spacewalk		Not Affected		CVE-2021-44228- Red Hat Customer Portal			Dec/21/2021
Red Hat	Red Hat JBoss Enterprise Application Platform Expansion Pack	7	Not Affected		CVE-2021-44228- Red Hat Customer Portal			Dec/20/2021
Red Hat Open- Stack Platform 13 (Queens)	opendaylight		Affected	No	CVE-2021-44228- Red Hat Customer Portal	End of Life		Dec/21/2021
Red5Pro RedGate					Red5Pro Link RedGate Link			
ResMed	myAir		Not Affected		ResMed Advisory Link			12/21/2021
ResMed	AirView		Not Affected		ResMed Advisory Link			12/21/2021
Redis Reiner SCT ReportURI					Redis Link Reiner SCT Forum ReportURI Link			
Respondus					Respondus	This		
					Support Link	advi- sory is		
						avail- able to		
						cus- tomers		
						only		
						and has not		
						been re- viewed		
						by CISA		
Revenera					Revenera /	CISII		
/ Flexera					Flexera Community Link			
Ricoh RingCentra	.1				Ricoh Link RingCentral			
	-				Security Bulletin			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Riverbed					Riverbed Support Link		
Rockwell Automatio	FactoryTalk n Analytics DataFlowML		Affected	Under development	PN1579 - Log4Shell Vulnerability Notice		12/15/2021
Rockwell Automatio	FactoryTalk n Analytics DataView	3.03.00	Affected	Under development	PN1579 - Log4Shell Vulnerability Notice		12/15/2021
Rockwell Automatio	Industrial n 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 Automatio	MES EIG	3.03.00	Affected	No, product discontinued	PN1579 - Log4Shell Vulnerability Notice	Customers should up- grade to EIG Hub if possi- ble or work with their local repre- senta- tives about alterna- tive solutions.	12/15/2021
Rockwell Automatio	VersaVirtual n	Series A	Fixed	Follow the mitigation instructions outlined by VMware in VMSA-2021-0028	PN1579 - Log4Shell Vulnerability Notice		12/15/2021
Rockwell Automatio	Warehouse n Management	4.01.00, 4.02.00, 4.02.01, 4.02.02	Affected	Under development	PN1579 - Log4Shell Vulnerability Notice		12/15/2021
Rollbar					Rollbar Blog Post		
Rosette.com	m				Rosette.com Support Link		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
RSA	SecurID		Not					
	Authentica-		Affected					
	tion							
	Manager							
RSA	SecurID		Not					
	Authentica-		Affected					
	tion							
	Manager							
	Prime							
RSA	SecurID		Not					
10011	Authentica-		Affected					
	tion		Miccoca					
	Manager							
	WebTier							
RSA	SecurID		Not					
пра	Gover-		Affected					
			Affected					
	nance and							
DCA	Lifecycle		NT 4					
RSA	SecurID		Not					
	Gover-		Affected					
	nance and							
	Lifecycle							
	Cloud							
RSA	SecurID		Not					
	Identity		Affected					
	Router							
RSA					RSA Netwitness			
${\bf Netwitness}$					Community Link			
Rstudioapi	Rstudioapi	0.13	Not		https://github.			12/21/2021
			Affected		com/rstudio/			
					rstudioapi			
Rubrik					Rubrik Support	This		
					Link	advi-		
						sory is		
						avail-		
						able to		
						cus-		
						tomers		
						only		
						and has		
						not		
						been re-		
						viewed		
						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 (sup- port.ruckuswirele			12/13/2021
RunDeck by PagerDuty	, ,				RunDeck Docs Link	,		

PagerDuty PagerDuty SaaS Fixed PagerDuty Log4j Ve cur- Zero-Day rently Vulnerability see no Updates evi- dence of com- pro- mises on our plat- form. Our teams con- tinue to moni- tor for new de- velop-
ments and for im- pacts on sub- processors and depen- dent sys- tems. Pager- Duty SaaS cus- tomers do not need to take any ad- ditional

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Runecast	Runecast	6.0.3	Fixed	Yes	Runecast Release			
	Analyzer				notes			
SAE-IT					SAE-IT News			
					Link			
SAFE					SAFE FME			
FME					Server			
Server					Community Link			
SAGE					SAGE			
					Announcement			
					Link			
SailPoint					SailPoint	This		
					Community Link	advi-		
					·	sory is		
						avail-		
						able to		
						cus-		
						tomers		
						only		
						and has		
						not		
						been re-		
						viewed		
						by		
						CISA		

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
alesforce	Analytics		Affected		Salesforce	"Analytics	12/15/2021
	Cloud				Statement	Cloud	
						is re-	
						ported	
						to be	
						af-	
						fected	
						by	
						CVE-	
						2021-	
						44228.	
						Ser-	
						vices	
						have	
						been	
						up-	
						dated	
						to miti-	
						gate	
						the	
						issues	
						identi-	
						fied in CVE-	
						2021-	
						44228	
						and we	
						and we are exe-	
						cuting	
						our final	
						valida-	
						tion	
						01011	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other Re	ferences	Last Updated
Salesforce	B2C		Affected		Salesforce	"B2C		12/15/2021
	Commerce				Statement	Com-		, ,
	Cloud					merce		
						Cloud		
						is re-		
						ported		
						to be		
						af-		
						fected		
						by		
						CVE-		
						2021-		
						44228.		
						The		
						service		
						is being		
						up-		
						dated		
						to		
						remedi-		
						ate the		
						vulner-		
						ability		
						identi-		
						fied in		
						CVE-		
						2021-		
						44228."		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updat
Salesforce	ClickSoftwar	e	Affected		Salesforce	"ClickSo	oftware	12/15/2021
	(As-a-				Statement	(As-a-		, ,
	Service)					Service))	
						is re-		
						ported		
						to be		
						af-		
						fected		
						by		
						CVE-		
						2021-		
						44228.		
						The		
						service		
						is being		
						up-		
						dated		
						to		
						remedi-		
						ate the		
						vulner-		
						ability		
						identi-		
						fied in		
						CVE-		
						2021-		
						44228."		
Salesforce	ClickSoftwar	e	Unknown		Salesforce	"Please		12/15/202
	(On-				Statement	contact		
	Premise)					Cus-		
						tomer	_	
						Support	. 77	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Salesforce	Community		Affected		Salesforce	"Commu	nity	12/15/2021
	Cloud				Statement	Cloud		
						is re-		
						ported		
						to be		
						af-		
						fected		
						by		
						CVE-		
						2021-		
						44228.		
						The		
						service		
						is being		
						up-		
						dated		
						to		
						remedi-		
						ate the		
						vulner-		
						ability		
						identi-		
						fied in		
						CVE-		
						2021-		
						44228."		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Salesforce	Data.com		Affected		Salesforce	"Data.com	12/15/2021
					Statement	is re-	
						ported	
						to be	
						af-	
						fected	
						by	
						ČVE-	
						2021-	
						44228.	
						The	
						service	
						has a	
						mitiga-	
						tion in	
						place	
						and is	
						being	
						up-	
						dated	
						to	
						remedi-	
						ate the	
						vulner-	
						ability	
						identi-	
						fied in	
						CVE-	
						2021-	
						44228."	
		<=53.0.0	Fixed		Vendor Link		12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Salesforce	Datorama		Affected		Salesforce	"Datoran	ıa	12/15/2021
					Statement	is re-		
						ported		
						to be		
						af-		
						fected		
						by		
						CVE-		
						2021-		
						44228.		
						The		
						service		
						has a		
						mitiga-		
						tion in		
						place		
						and is		
						being		
						up-		
						dated		
						to		
						remedi-		
						ate the		
						vulner-		
						ability		
						identi-		
						fied in		
						CVE-		
						2021-		
						44228."		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Salesforce	Evergage		Affected		Salesforce	"Evergage	12/15/2021
	(Interac-				Statement	(Inter-	• •
	tion					action	
	Studio)					Studio)	
						is re-	
						ported	
						to be	
						af-	
						fected	
						by	
						CVE-	
						2021-	
						44228.	
						Ser-	
						vices	
						have	
						been	
						up-	
						dated	
						to miti-	
						gate	
						the	
						issues	
						identi-	
						fied in	
						CVE-	
						2021-	
						44228	
						and we	
						are exe-	
						cuting	
						our	
						final	
						valida-	
						tion	
						steps."	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Salesforce	Force.com		Affected		Salesforce Statement	"Force.com is reported to be affected by CVE- 2021- 44228. The service is being up- dated to remediate the vulner- ability identi- fied in CVE- 2021-	12/15/2021
Salesforce	Heroku		Not Affected		Salesforce Statement	44228." "Heroku is reported to not be affected by CVE- 2021- 44228; no further action is necessary at this time."	12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Salesforce	Marketing Cloud		Affected		Salesforce Statement	"Market	ing	12/15/2021
	Cloud				Statement	is re-		
						ported		
						to be		
						af-		
						fected		
						by		
						CVE-		
						2021-		
						44228.		
						The		
						service		
						is being		
						up-		
						dated		
						to		
						remedi-		
						ate the		
						vulner-		
						ability		
						identi-		
						fied in		
						CVE-		
						2021-		
						44228."		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Salesforce	MuleSoft		Affected		Salesforce	"MuleSot	ft	12/15/2021
	(Cloud)				Statement	(Cloud)		
						is re-		
						ported		
						to be		
						af-		
						fected		
						by		
						CVE-		
						2021-		
						44228.		
						The		
						service		
						is being		
						up-		
						dated		
						to		
						remedi-		
						ate the		
						vulner-		
						ability		
						identi-		
						fied in		
						CVE-		
						2021-		
						44228."		
Salesforce	MuleSoft		Unknown		Salesforce	"Please		12/15/2021
	(On-				Statement	contact		
	Premise)					Cus-		
						tomer		
						Support.	,,,	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Salesforce	Pardot		Affected		Salesforce	"Pardot	12/15/2021
					Statement	is re-	
						ported	
						to be	
						af-	
						fected	
						by	
						CVE-	
						2021-	
						44228.	
						The	
						service	
						is being	
						up-	
						dated	
						to	
						remedi-	
						ate the	
						vulner-	
						ability	
						identi-	
						fied in	
						CVE-	
						2021-	
						44228."	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Salesforce	Sales Cloud		Affected		Salesforce	"Sales		12/15/2021
					Statement	Cloud		, ,
						is re-		
						ported		
						to be		
						af-		
						fected		
						by		
						CVE-		
						2021-		
						44228.		
						The		
						service		
						is being		
						up-		
						dated		
						to		
						remedi-		
						ate the		
						vulner-		
						ability		
						identi-		
						fied in		
						CVE-		
						2021-		
						44228."		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Salesforce	Service		Affected		Salesforce	"Service		12/15/2021
	Cloud				Statement	Cloud		, ,
						is re-		
						ported		
						to be		
						af-		
						fected		
						by		
						CVE-		
						2021-		
						44228.		
						The		
						service		
						is being		
						up-		
						dated		
						to		
						remedi-		
						ate the		
						vulner-		
						ability		
						identi-		
						fied in		
						CVE-		
						2021-		
						44228."		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Salesforce	Slack		Affected		Salesforce	"Slack		12/15/2021
					Statement	is re-		
						ported		
						to be		
						af-		
						fected		
						by		
						CVE-		
						2021-		
						44228.		
						The		
						service		
						has a		
						mitiga-		
						tion in		
						place		
						and is		
						being		
						up-		
						dated		
						to		
						remedi-		
						ate the		
						vulner-		
						ability		
						identi-		
						fied in		
						CVE-		
						2021-		
						44228."		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Update
Salesforce	Social		Affected		Salesforce	"Social		12/15/2021
	Studio				Statement	Studio		
						is re-		
						ported		
						to be		
						af-		
						fected		
						by		
						CVE-		
						2021-		
						44228.		
						The		
						service		
						has a		
						mitiga-		
						tion in		
						place		
						and is		
						being		
						up-		
						dated		
						to		
						remedi-		
						ate the		
						vulner-		
						ability		
						identi-		
						fied in		
						CVE-		
						2021-		
						44228."		
Salesforce	Tableau	< 2021.4.1	Fixed		Salesforce	Fixed		12/16/2021
	(On-				Statement	in		
	Premise)					2021.4.1		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Salesforce	Tableau (Online)		Affected		Salesforce Statement	"Tableau (On-line) is reported to be affected by CVE-2021-44228. The service is being updated to remediate the vulnerability identified in CVE-2021-44228."		12/15/2021
Sangoma					Sangoma Community Link	44220.		
SAP					https://support. sap.com/ content/dam/ support/en_us/ library/ssp/my- support/trust- center/sap-tc-01- 5025.pdf	This advisory is available to customers only and has not been reviewed by CISA		12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
SAP Ad-					SAP Advanced	This		12/17/2021
vanced					Platform	advi-		
Platform					Support Link	sory is		
						avail-		
						able to		
						cus-		
						tomers		
						only		
						and has		
						not		
						been re-		
						viewed		
						by		
~ . . .					GT TT 0004 44000	CISA		10/15/0001
SAP					CVE-2021-44228	The		12/17/2021
BusinessO	bjects				- Impact of Log4j	support		
					vulnerability on	docu-		
					SAP	ment is		
					BusinessObjects	avail-		
					SAP	able to		
					BusinessObjects	cus-		
					Support Link	tomers		
						only		
						and has		
						not		
						been re-		
						viewed		
						by		
O A O					0.0.0.0	CISA		
SAS					SAS Support Link			
SASSAFR	AC				SASSAFRAS			
SASSAFR	AS				Link			
Savignano					Savignano Link			
savignano software					Savigilano Link			
software solutions								
	SBT	<1 5 G	Affected	Voc	Release 1.5.7			19/15/9091
SBT	SDI	<1.5.6	Affected	Yes		.)		12/15/2021
					sbt/sbt(github.com	1)		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
ScaleComp	outing				ScaleComputing Community Link	This advisory is available to customers only and has not been reviewed by		
ScaleFusion Mobile- Lock Pro	n				ScaleFusion MobileLock Pro Help	CISA		
Schneider Electric	EcoStruxure IT Gateway	V1.5.0 to V1.13.0	Fixed	Yes	EcoStruxure Link			12/20/2021
Schneider Electric	EcoStruxure IT Expert	Cloud	Fixed	Yes				12/20/2021
Schneider Electric	Facility Expert Small Business	Cloud	Fixed	Yes	SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	Wiser by SE platform	Cloud	Fixed	Yes				12/20/2021
Schneider Electric	EASYFIT	Current software and earlier	Affected		SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	Ecoreal XL	Current software and earlier	Affected		SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	Eurotherm Data Reviewer	V3.0.2 and prior	Affected		SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	MSE	Current software and earlier	Affected		SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	NetBotz750/	755oftware versions 5.0 through 5.3.0	Affected		SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	NEW630	Current software and earlier	Affected		SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	SDK BOM	Current software and earlier	Affected		SE Cybersecurity Best Practices			12/20/2021
Schneider Electric	SDK- Docgen	Current software and earlier	Affected		SE Cybersecurity Best Practices			12/20/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Schneider	SDK-TNC	Current software	Affected		SE Cybersecurity			12/20/2021
Electric		and earlier			Best Practices			1 -1 -
Schneider	SDK-UMS	Current software	Affected		SE Cybersecurity			12/20/2021
Electric		and earlier			Best Practices			, ,
Schneider	SDK3D2DRe	en Cerer ent software	Affected		SE Cybersecurity			12/20/2021
Electric		and earlier			Best Practices			, ,
Schneider	SDK3D360W	idgetrent software	Affected		SE Cybersecurity			12/20/2021
Electric		and earlier			Best Practices			
Schneider	Select and	Current software	Affected		SE Cybersecurity			12/20/2021
Electric	Config	and earlier			Best Practices			
	DATA							
Schneider	SNC-API	Current software	Affected		SE Cybersecurity			12/20/2021
Electric		and earlier			Best Practices			
Schneider	SNC-CMM	Current software	Affected		SE Cybersecurity			12/20/2021
Electric		and earlier			Best Practices			
Schneider	SNCSEMTE	CHurrent software	Affected		SE Cybersecurity			12/20/2021
Electric		and earlier			Best Practices			
Schneider	SPIMV3	Current software	Affected		SE Cybersecurity			12/20/2021
Electric		and earlier			Best Practices			
Schneider	SWBEditor	Current software	Affected		SE Cybersecurity			12/20/2021
Electric		and earlier			Best Practices			
Schneider	SWBEngine	Current software	Affected		SE Cybersecurity			12/20/2021
Electric		and earlier			Best Practices			
Schweitzer			Not		SEL Advisory			12/21/2021
Engineer-			Affected		Link			
ing								
Laboratorie	es							
SCM					SCM Manager			
Manager					Link			
ScreenBear	n				ScreenBeam			
~					Article			
SDL					SDL worldServer			
worldServe	r				Link			
Seagull					Seagull Scientific			
Scientific					Support Link			
SecurePoin	t				SecurePoint			
					News Link			
Security					Security Onion			
Onion					Blog Post			

Desk Link Advisory is ava-	Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Desk Link Advisory is Sory is	Seeburger					Seeburger Service	This		
All							advi-		
A							sory is		
Cus- Community Community							ava-		
tomers only and has not been re- viewed by CISA cry cry cry cry cry cry cry cry cry cr							iable to		
only and has not been reviewed by CISA CISA							cus-		
and has not been reviewed by CISA Sentine One Sentine One Blog Post							tomers		
Not Sentine One Sentine One Blog Post							only		
been reviewed by CISA cinelOne SentinelOne Blog Post Sentry Blog Post SEP Support Link rer Server Eye Blog Post Server Eye Blog Post ServiceNow Support Link Shibboleth Announcement Shibboleth Announcement All Identity Not Log4j CVE 12/10/2021 pify Froducts Provider>=3.0, Affected (non)-impact Froducts Software versions pify Shopify Community Link SentinelOne Blog Post SentinelOne Blog Post Sentry Blog Post Server Eye Blog Post Server Eye Blog Post ServiceNow Support Link Shibboleth Announcement Shibboleth Announcement Shibboleth									
viewed by CISA cinelOne cinelOne cry cry cry cry cry cry cry cr							not		
by CISA SentinelOne Blog Post Serty Blog Post SEP Support Link Server Eye Blog Post ServiceNow ServiceNow Soboleth All Identity Products Products Products Products Products Products Products ServiceNow Support Link Shibboleth Announcement Log4j CVE Log4j CVE Log4j CVE Log4j CVE Log4j CVE Log4j CVE ServiceNow Support Link Shibboleth Announcement Shibboleth Shibboleth Announcement Shibboleth Shibboleth Shibboleth Announcement Shibboleth							been re-		
CISA CinelOne CinelOne Ciry Ciry Ciry Ciry Ciry Ciry Ciry Ciry							viewed		
SentinelOne Blog Post Sentry Blog Post SEP Support Link For Server Eye Blog Post Server Eye Blog Post Server Eye Blog Post Server Eye Blog Post ServiceNow Support Link Shibboleth Announcement Sholeth All Identity Products Products Products Products Software versions Shopify Community Link							by		
Post Sentry Blog Post SEP Support Link For Server Eye Blog Post ServiceNow FiceNow Fic							CISA		
Sentry Blog Post SEP Support Link For Server Eye Blog Post ServiceNow ServiceNow Support Link Soboleth All Identity Products Products Products Products ServiceNom Affected Affected Affected Affected Affected ServiceNom Support Link Shibboleth Announcement Log4j CVE (non)-impact Shopify Community Link	SentinelOr	ne				SentinelOne Blog			
SEP Support Link For Server Eye Blog Post ServiceNow Support Link Support Link Shibboleth Announcement Log4j CVE Products Provider>=3.0, Affected All other software versions Pify Sibopify Community Link						Post			
Link Server Eye Blog Post ServiceNow ServiceNow Support Link Shibboleth Announcement Sholeth All Identity Products Provider>=3.0, Affected All other Software versions pify Service Eye Blog Post ServiceNow Support Link Shibboleth Announcement (non)-impact Shopify Community Link	Sentry								
Server Eye Blog Post SiceNow SiceNow Support Link Shibboleth Announcement Sholeth Products Products Provider>=3.0, Affected All other Software versions Service Row ServiceNow Support Link Shibboleth Announcement Log4j CVE (non)-impact Shopify Community Link	EP					SEP Support			
Post ServiceNow Support Link Support Link Shibboleth Announcement Log4j CVE Products Products Provider>=3.0, Affected All other software versions Pify Shopify Community Link						Link			
ServiceNow Support Link Support Link Shibboleth Announcement Sholeth All Identity Not Log4j CVE 12/10/2021 Products Provider>=3.0, Affected (non)-impact All other software versions Pify Shopify Community Link	erver								
Support Link Shibboleth Shibboleth Announcement Log4j CVE Products Provider>=3.0, Affected All other software versions Shopify Community Link	Eye								
Shibboleth Announcement boleth All Identity Not Log4j CVE 12/10/2021 Products Provider>=3.0, Affected (non)-impact All other software versions pify Shibboleth Announcement Log4j CVE (non)-impact Shopify Community Link	ServiceNov	V							
Announcement Log4j CVE Products Products Provider>=3.0, Affected All other software versions Shopify Community Link									
bboleth All Identity Not Log4j CVE 12/10/2021 Products Provider>=3.0, Affected (non)-impact All other software versions pify Shopify Community Link	Shibboleth	l				Shibboleth			
Products Provider>=3.0, Affected (non)-impact All other software versions pify Shopify Community Link									
All other software versions pify Community Link	shibboleth								12/10/2021
software versions pify Shopify Community Link		Products		Affected		(non)-impact			
pify Shopify Community Link									
Community Link			software versions						
	Shopify								
Siebel Link									
	Siebel					Siebel Link			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Advantage Navigator Energy & Sustainability	All Versions <2021-12-13	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Vulnerability CVE 2021- 44228 fixed on central cloud service start- ing 2021- 12-13; no user actions neces- sary. See further recom- menda- tions from Siemens Advi- sory SSA-	12/18/2021
Siemens	Advantage Navigator Software Proxy	All Versions	Affected	No	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Currently no remediation is available. See further recommendations from Siemens Advisory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Vendor Siemens	Product Capital	Version(s) All Versions>=2019.1 SP1912 only if Teamcenter integration feature is used	Status Affected	Update Available No	Vendor Link Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Only affected if Team- center integra- tion feature is used. Cur- rently no remedi- ation is avail- able. Find de- tailed mitiga- tions steps at:Mitigations Link; See further recom- menda- tions from Siemens Advi-	Last Updated 12/18/2021
						sory	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Cerberus DMS	V5.0, V5.1 with Advanced Reporting EM installed	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Remove the JndiLookup class from the class- path. De- tailed instruc- tions are avail- able here. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

ndor Product	Version(s)	Status	Update Available	Vendor Link	Notes Othe	er References	Last Updated
mens Comos Desktop App	Version(s) All Versions	Status Affected	Update Available No	Vendor Link Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Notes Other Currently no remediation is available. Uninstall "Teamcenter Client Communication System (TCSS)" or block both incoming and outgoing connections between the system and the Internet. See further recommendations from Siemens	r References	Last Updated 12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Desigo CC	V3.0, V4.0, V4.1, V4.2 with Advanced Reporting EM installed	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Remove the JndiLookup class from the class- path. De- tailed instruc- tions are avail- able here. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Desigo CC	V5.0, 5.1 with Advanced Reporting OR Info Center EM installed	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Remove the JndiLookup class from the class- path. De- tailed instruc- tions are avail- able here. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens	E-Car OC Cloud Application	All Versions <2021-12-13	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Vulneral CVE 2021- 44228 fixed on central cloud service start- ing 2021- 12-13; no user actions neces- sary. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	pility	12/18/2021

Vendor .	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens	Energy	V3.1	Affected	Yes	Siemens Advisory	Find		12/18/2021
	Engage				- SSA-661257:	de-		
					Apache Log4j	tailed		
					Vulnerabilities	remedi-		
						ation		
						and		
						mitiga-		
						tion		
						infor-		
					mation			
					on the			
					Ener-			
						gyIP		
						docs		
						portal.		
						See		
						further		
						recom-		
						menda-		
						tions		
						from		
						Siemens		
						Advi-		
						sory		
						SSA-		
						661257		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens	EnergyIP	V8.5, V8.6, V8.7,	Affected	Yes	Siemens Advisory	Note:		12/18/2021
		V9.0			- SSA-661257:	Ener-		
					Apache Log4j	gyIP		
					Vulnerabilities	V8.5		
						and		
						V8.6		
						applica-		
						tions		
						are not		
						directly		
						af-		
						fected,		
						but CAS is.		
						Find		
						de-		
						tailed		
						remedi-		
					ation			
					and			
						mitiga-		
						tion		
						infor-		
						mation		
						on the		
						Ener-		
						gyIP		
						docs		
						portal.		
						See		
						further		
						recom-		
						menda-		
						tions		
						from		
						Siemens		
						Advi-		
						sory		
						SSA-		
						661257		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
emens	EnergyIP	V3.7. V3.8	Affected	Yes	Siemens Advisory	Specific		12/18/2021
	Prepay				- SSA-661257:	mitiga-		
					Apache Log4j	tion		
					Vulnerabilities	infor-		
						mation		
						has		
						been re-		
						leased		
					for the			
						cus-		
						tomer		
						projects		
						with		
					the			
						request		
						of		
						imme-		
						diate		
					deploy-			
						ment.		
						The		
						long-		
						term		
						solu-		
						tion of		
						updat-		
						ing the		
						log4j2		
						compo-		
						nent to		
						a fix		
						version		
						is being		
						tested		
						and		
						will be		
						re-		
						leased,		
						once		
						con-		
						firmed		
						being		
						safe for		
						the par-		
						ticular		
						prod-		
						uct .		
						version		
						in line		
					415	with		
						the		
						project		
						Service		
						Level		
						Agree-		
						ments.		
						See		
						further		
						recom-		
						menda-		

menda-

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Vendor Siemens	Product Enlightened Amaze	Version(s) All Versions <2021-12-10	Affected	Yes Yes	Vendor Link Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Vulnerable fixed on central cloud services starting 2021-12-10; no user actions necessary. For Comfy and Enlighted, see the Additional Information section and further recommendations from Siemens Advisory SSA-661257		12/18/2021

Where <2021-12-11	SSA-661257: Apache Log4j Vulnerabilities	Vulnerabilities fixed on central cloud services start- ing 2021- 12-11; no user actions neces- sary. For Comfy and En- lighted, see the	12/18/2021
		Additional Information section and further recommendations from Siemens Advi-	
		Siemens Advi- sory	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Geolus Shape Search V10	All Versions	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Remove the JndiLookup class from the class- path. Find de- tailed remedi- ation and mitiga- tion infor- mation here. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Geolus Shape Search V11	All Version	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Remove the JndiLookup class from the class- path. Find de- tailed remedi- ation and mitiga- tion infor- mation here. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens	GMA-	All Version	Affected	Yes	Siemens Advisory	Update		12/18/2021
	Manager	>=V8.6.2j-398			- SSA-661257:	to		
		and $<$ V8.6.2-472			Apache Log4j	V8.6.2-		
					Vulnerabilities	472 or		
						later		
						version.		
						Block		
						both in-		
						coming		
						and		
						outgo-		
						ing connec-		
						tions		
						be-		
						tween		
						the		
						system		
						and the		
						Inter-		
						net.		
						See		
						further		
						recom-		
						menda-		
						tions		
						from		
						Siemens		
						Advi-		
						sory		
						SSA-		
						661257		

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes (Other References	Last Updated
iemens	HES UDIS	All Versions	Affected	No	Siemens Advisory	Currently		12/18/2021
					- SSA-661257:	no		
					Apache Log4j	remedi-		
					Vulnerabilities	ation is		
						avail-		
						able.		
						Specific		
						mitiga-		
						tion		
						infor-		
						mation		
						has		
						been re-		
						leased		
						for the		
						local		
						project		
						teams		
						with		
						the		
						request		
						of		
						imme-		
						diate		
						deploy-		
						ment.		
						A		
						patch is		
						planned		
						for the		
						next		
						regular		
						release.		
						See		
						further		
						recom-		
						menda-		
						tions		
						from		
						Siemens		
						Advi-		
						sory		
						SSA-		
						661257		

Siemens Industrial All Versions Affected Yes Edge Management App (IEM-App)	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Exposure to vulner- ability is limited as IEM- App runs in	12/18/2021
		IEM- OS and IEM- OS is not in- tended to be ex- posed to public inter- net and should be oper- ated in a pro- tected envi- ron- ment. Please refer to the In- dustrial Edge - Secu- rity overview. See further recom- menda- tions from	
		tions from Siemens Advi- sory SSA-	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens	Industrial Edge Man- agement Hub	All versions <2021-12-13	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Vulneral CVE- 2021- 44228 fixed on central cloud service start- ing 2021- 12-13; no user actions neces- sary. See further recom- menda- tions from Siemens Advi- sory SSA- 661257		12/18/2021

dor P	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
nens Ir E aş O	Product Industrial Edge Management OS IEM-OS)	Version(s) All Versions	Status Affected	Yes Yes	Vendor Link Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Exposure to vulner-ability is limited as IEM-OS is not intended to be exposed to public internet and should be operated in a protected environment. Please refer to the Industrial Edge - Security overview See further recommendations from		Last Updated 12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens	LOGO! Soft Comfort	All versions	Not Affected		Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Note: LOGO! Soft Comfort products were previously listed as affected. They were removed after closer investigation showed that they are not affected.		12/18/2021

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
ndor mens	Product Mendix Applications	Version(s) All Versions	Status Affected (See Notes)	Update Available Yes	Vendor Link Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Notes Although the Mendix runtime itself is not vulnerable to this exploit, we nevertheless recommend to upgrade log4j-core to the latest available version if log4j-core is part of your project. This advice is regardless of the JRE/JDF version the app runs on. See		Last Updated 12/18/2021
					426	State- ment for more details. See further recom- menda- tions from Siemens Advi- sory SSA- 661257		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	MindSphere App Man- agement Cockpits (Developer & Operator)	All Versions <2021-12-16	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Vulnerabilities fixed with update on 2021- 12-16; no user actions neces- sary. See further recom- menda- tions from Siemens Advi- sory SSA-	12/18/2021
Siemens	MindSphere Asset Manager	All Versions <2021-12-16	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Vulnerabilities fixed with update on 2021- 12-16; no user actions neces- sary. See further recom- menda- tions from Siemens Advi- sory SSA-	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	MindSphere Cloud Platform	All Versions <2021-12-11	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Vulnerabilities fixed on central cloud service start- ing 2021- 12-11; no user actions neces- sary. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021
Siemens	MindSphere IAM (User Management	All Versions (/Settings)	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Vulnerabilities fixed with update on 2021- 12-16; no user actions neces- sary. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	MindSphere Integrated Data Lake	All Versions <2021-12-16	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Vulnerabilities fixed with update on 2021- 12-16; no user actions neces- sary. See further recom- menda- tions from Siemens Advi- sory SSA-	12/18/2021
Siemens	MindSphere Notifica- tion Service	All Versions <2021-12-16	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Vulnerabilities fixed with update on 2021- 12-16; no user actions neces- sary. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	MindSphere Predictive Learning	All Versions	Affected	No	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Currently no remedi- ation is avail- able. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021
Siemens	MindSphere Usage Trans- parency Service	All Versions <2021-12-16	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Vulnerabilities fixed with update on 2021- 12-16; no user actions neces- sary. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
ndor mens	Product MindSphere Visual Explorer		Status Affected	Update Available No	Vendor Link Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Currently no remediation is avail- able. Al- though Mind- Sphere Visual Ex- plorer does not use the af- fected component directly it is in- cluded within the in- cluded third- party component Tableau. While the re- garding interac- tion with Tableau is deac- tivated, a reme-		Last Updated 12/18/2021
						tivated, a remediating patch for Tableau is still awaited. See further recom-		
					432	menda- tions from Siemens Advi- sory SSA- 661257		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens	NX	All Versions	Affected	No	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Currently no remediation is available. Find detailed mitigation steps here. See further recommendations from Siemens Advisory SSA-		12/18/2021
Siemens	Opcenter EX CP Process Au- tomation Control	All versions >=V17.2.3 and <v18.1< td=""><td>Affected</td><td>Yes</td><td>Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities</td><td>661257 Update to V18.1 or later version to fix CVE- 2021- 44228. See further recom- menda- tions from Siemens Advi- sory SSA- 661257</td><td></td><td>12/18/2021</td></v18.1<>	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	661257 Update to V18.1 or later version to fix CVE- 2021- 44228. See further recom- menda- tions from Siemens Advi- sory SSA- 661257		12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens	Opcenter Intelligence	All Versions >=V3.2 only OEM version that ships Tableau	Affected	No	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Currently no remediation is available. See further recommendations from Siemens Advisory SSA-661257	y	12/18/2021

Vendor Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Vendor Product Siemens Operation Scheduler	All versions	Status Affected	Update Available No	Vendor Link Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Notes Currently no remediation is available. Block both incoming and outgoing connections between the system and the Internet. See further recommendations from Siemens Advi-		Last Updated 12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Vendor Siemens	Product SENTRON powerman- ager V4	Version(s) V4.1, V4.2	Status Affected	Update Available No	Vendor Link Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Currently no remediation is avail- able. Block both in- coming and outgo- ing connections be- tween the system and the Inter- net. See further recom- menda- tions		Last Updated 12/18/2021
						tions from Siemens Advi- sory		
						sory SSA- 661257		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens	SIGUARD DSA	V4.2, 4.3, 4.4	Affected	No	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Currently no remedi- ation is avail- able. See further recom- menda- tions from Siemens Advi- sory SSA- 661257		12/18/2021
Siemens	SIMATIC WinCC	All Versions	Not Affected		Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	SIMATI WinCC products were previously listed as affected. They were removed after closer investigation showed that they are not affected.		12/18/2021

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
liemens	Simcenter	All Versions	Affected	Yes	Siemens Advisory	Remove	12/18/2021
	3D	<=V022.1			- SSA-661257:	the	
					Apache Log4j	JndiLookup	
					Vulnerabilities	class	
						from	
						the	
						class-	
						path.	
						Find	
						de-	
						tailed	
						remedi-	
						ation	
						and	
					mitiga-		
						tion	
						infor-	
						mation	
						here.	
						See	
						further	
						recom-	
						menda-	
						tions	
						from	
						Siemens	
						Advi-	
						sory	
						SSA-	
						661257	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Vendor Siemens	SiPass integrated V2.80	Version(s) All Versions	Status Affected	No	Vendor Link Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Currently no remediation is available. Block both incoming and outgoing connections betwen the system and the Internet.See further recommendations from Siemens Advisory SSA-	12/18/2021

/endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	SiPass	All Versions	Affected	No	Siemens Advisory	Currently	12/18/2021
	integrated				- SSA-661257:	no	
	V2.85				Apache Log4j	remedi-	
					Vulnerabilities	ation is	
						avail-	
						able.	
						Block	
						both in-	
						coming	
						and	
						outgo-	
						ing	
						connec-	
						tions	
						betwen	
						the	
						system	
						and the	
						Inter-	
						net.	
						See	
						further	
						recom-	
						menda-	
						tions	
						from	
						Siemens	
						Advi-	
						sory	
						SSA-	
						661257	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes O	ther References	Last Updated	
liemens	Siveillance	All Versions	Affected	No	Siemens Advisory	Currently		12/18/2021	
	Command	>=4.16.2.1			- SSA-661257:	no			
					Apache Log4j	remedi-			
					Vulnerabilities	ation is			
						avail-			
						able.			
						Block			
						both in-			
						coming			
						and			
						outgo-			
						ing			
						connec-			
						tions			
							betwen		
						the			
						system and the			
						Inter-			
						net.			
						See			
						further			
						recom-			
						menda-			
						tions			
						from			
						Siemens			
						Advi-			
						sory			
						SSA-			
						661257			

Vendor (Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
iemens	Siveillance	All Versions	Affected	Yes	Siemens Advisory	Hotfix		12/18/2021
	Control				- SSA-661257:	avail-		
	Pro				Apache Log4j	able for		
					Vulnerabilities	ver-		
						sions		
						>=		
						V2.1		
						(please		
						contact		
						cus-		
						tomer		
						sup-		
						port). Block		
						both in-		
						coming		
					and			
						outgo-		
						ing		
						connec-		
						tions		
						betwen		
						the		
						system		
						and the		
						Inter-		
						net.See		
						further		
						recom-		
						menda-		
						tions		
						from		
						Siemens		
						Advi-		
						sory		
						SSÅ-		
						661257		

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
iemens	Siveillance	All Versions	Affected	No	Siemens Advisory	Currently	12/18/2021
	Identity				- SSA-661257:	no	
	V1.5				Apache Log4j	remedi-	
					Vulnerabilities	ation is	
						avail-	
						able.	
						Block	
						both in-	
						coming	
						and	
						outgo-	
						ing	
						connec-	
						tions	
						betwen	
						the	
						system	
						and the	
						Inter-	
						net.	
						See	
						further	
						recom-	
						menda-	
						tions	
						from	
						Siemens	
						Advi-	
						sory	
						SSA-	
						661257	

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
iemens	Siveillance	All Versions	Affected	No	Siemens Advisory	Currently	12/18/2021
	Identity				- SSA-661257:	no	
	V1.6				Apache Log4j	remedi-	
					Vulnerabilities	ation is	
						avail-	
						able.	
						Block	
						both in-	
						coming	
						and	
						outgo-	
						ing	
						connec-	
						tions	
					betwen		
						the	
						system	
						and the	
						Inter-	
						net.	
						See	
						further	
						recom-	
						menda-	
						tions	
						from	
						Siemens	
						Advi-	
						sory	
						SSA-	
						661257	

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Othe	er References	Last Updated
liemens	Siveillance	All Versions	Affected	No	Siemens Advisory	Currently		12/18/2021
	Vantage				- SSA-661257:	no		
					Apache Log4j	remedi-		
					Vulnerabilities	ation is		
						avail-		
						able.		
						Block		
						both in-		
					coming			
						and		
					outgo-			
						ing		
						connec- tions		
						betwen		
						the		
					system			
						and the		
						Inter-		
						net.		
						See		
						further		
						recom-		
						menda-		
						tions		
						from		
						Siemens		
						Advi-		
						sory		
						SSA-		
						661257		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Solid Edge CAM Pro	All Versions delivered with Solid Edge SE 2020 or later version	Affected	No No	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Currently no remediation is available. See further recommendations from Siemens Advisory SSA- 661257	12/18/2021
Siemens	Solid Edge Harness Design	All Versions >=2020 SP2002 only if Teamcenter integration feature is used	Affected	No	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Currently no remediation is available. Find detailed mitigation steps here. See further recommendations from Siemens Advisory SSA- 661257	12/18/2021

Vendor	Product Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens	Spectrum All versions Power 4 >=V4.70 SP8	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Update to V4.70 SP9 and apply the patch pro- vided via cus- tomer sup- port. See further recom- menda- tions from Siemens Advi- sory SSA-	Other recremes	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens	Spectrum Power 7	All Versions >=V2.30 SP2	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Update to V21Q4 and apply the patch provided via customer support. See further recommendations from Siemens Advisory SSA-661257		12/18/2021

Vendor (Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens	Teamcenter	All Versions	Affected	Yes	Siemens Advisory	Remove		12/18/2021
		>=V13.1			- SSA-661257:	the		
					Apache Log4j	JndiLool	kup	
					Vulnerabilities	class		
						from		
						the		
						class-		
						path.		
						Find		
						de-		
						tailed		
						remedi-		
						ation		
						and		
						mitiga-		
						tion		
						infor-		
						mation		
						here.		
						See		
						further		
						recom-		
						menda-		
						tions		
						from		
						Siemens		
						Advi-		
						sory		
						SSA-		
						661257		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Teamcenter Active Workspace	All Versions >=V4.3	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Remove the JndiLookup class from the class- path. Find de- tailed remedi- ation and mitiga- tion infor- mation here. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Teamcenter Briefcase Browser	All Versions >=V13.1	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Remove the JndiLookup class from the class- path. Find de- tailed remedi- ation and mitiga- tion infor- mation here. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Teamcenter Data Share Manager	All Versions >=V13.1	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Remove the JndiLookup class from the class- path. Find de- tailed remedi- ation and mitiga- tion infor- mation here. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Teamcenter Deploy- ment Center	All Versions >=V13.1	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Remove the JndiLookup class from the class- path. Find de- tailed remedi- ation and mitiga- tion infor- mation here. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Teamcenter Dispatcher Service	All Versions >=V13.1	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Remove the JndiLookup class from the class- path. Find de- tailed remedi- ation and mitiga- tion infor- mation here. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Teamcenter EDA	All Versions >=V2.3	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Remove the JndiLookup class from the class- path. Find de- tailed remedi- ation and mitiga- tion infor- mation here. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Teamcenter FMS	All Versions >=V11.3	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Remove the JndiLookup class from the class- path. Find de- tailed remedi- ation and mitiga- tion infor- mation here. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
iemens	Teamcenter Integration Framework	All Versions >=V13.2	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Remove the JndiLookup class from the class- path. Find de- tailed remedi- ation and mitiga- tion infor- mation here. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Teamcenter MBSE Gateway	All Versions >=V4.0	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Remove the JndiLookup class from the class- path. Find de- tailed remedi- ation and mitiga- tion infor- mation here. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Teamcenter Mendix Connector	V1.0	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Remove the JndiLookup class from the class- path. Find de- tailed remedi- ation and mitiga- tion infor- mation here. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Teamcenter Microser- vices Framework	All Versions >=V5.1	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Remove the JndiLookup class from the class- path. Find de- tailed remedi- ation and mitiga- tion infor- mation here. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Teamcenter Polarion Integration	All Versions >=V5.1	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Remove the JndiLookup class from the class- path. Find de- tailed remedi- ation and mitiga- tion infor- mation here. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
siemens	Teamcenter Rapid Start	All Versions >=V13.1	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Remove the JndiLookup class from the class- path. Find de- tailed remedi- ation and mitiga- tion infor- mation here. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Teamcenter Reporting and Analytics	All Versions based on Java SOA client >=V11.3	Affected	Yes Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Remove the JndiLookup class from the class- path. Find de- tailed remedi- ation and mitiga- tion infor- mation here. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Teamcenter Require- ments Integrator	All Versions based on Java SOA client >=V11.3	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Remove the JndiLookup class from the class- path. Find de- tailed remedi- ation and mitiga- tion infor- mation here. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Teamcenter Retail Footwear and Apparel	All Versions >=V4.3	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Remove the JndiLookup class from the class- path. Find de- tailed remedi- ation and mitiga- tion infor- mation here. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens	Teamcenter	All Versions	Affected	Yes	Siemens Advisory	Remove		12/18/2021
	Security	>=V11.3			- SSA-661257:	the		
	Services				Apache Log4j	JndiLool	kup	
					Vulnerabilities	class		
						from		
						the		
						class-		
						path.		
						Find		
						de-		
						tailed		
						remedi-		
						ation		
						and		
						mitiga-		
						tion		
						infor-		
						mation		
						here.		
						See		
						further		
						recom-		
						menda-		
						tions		
						from		
						Siemens		
						Advi-		
						sory		
						SSA-		
						661257		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Teamcenter Supplier Collaboration	All Versions >=V5.1	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Remove the JndiLookup class from the class- path. Find de- tailed remedi- ation and mitiga- tion infor- mation here. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Teamcenter System Modeling Workbench	All Versions based on Java SOA client >=V11.3	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Remove the JndiLookup class from the class- path. Find de- tailed remedi- ation and mitiga- tion infor- mation here. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Teamcenter Technical Publishing	All Versions >=V2.10	Affected	Yes	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Remove the JndiLookup class from the class- path. Find de- tailed remedi- ation and mitiga- tion infor- mation here. See further recom- menda- tions from Siemens Advi- sory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens	VeSys	All Versions	Affected	No	Siemens Advisory	Currently	y	12/18/2021
		>=2019.1			- SSA-661257:	no		, ,
		SP1912 only if			Apache Log4j	remedi-		
		Teamcenter			Vulnerabilities	ation is		
		integration				avail-		
		feature is used				able.		
					Find	Find		
						de-		
						tailed		
						mitiga-		
						tion		
						steps		
						here.		
						See		
						further		
						recom-		
						menda-		
						tions		
						from		
						Siemens		
						Advi-		
						sory		
						SSA-		
						661257		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Xpedition Enterprise	All Versions >=VX.2.6	Affected	No No	Siemens Advisory - SSA-661257: Apache Log4j Vulnerabilities	Currently no remediation is available. Find detailed mitigation steps here. See further recommendations from Siemens Advisory SSA- 661257	12/18/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens	Xpedition	All Versions	Affected	No	Siemens Advisory	Currently	У	12/18/2021
	IC	>=VX.2.6			- SSA-661257:	no		
	Packaging				Apache Log4j	remedi-		
					Vulnerabilities	ation is		
						avail-		
						able.		
						Find		
					de-			
					tailed			
						mitiga-		
						tion		
						steps		
						here.		
						See		
						further		
						recom-		
						menda-		
						tions		
						from		
						Siemens		
						Advi-		
						sory		
						SSA-		
						661257.		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	ATELLICA		Affected	See Notes	Siemens	If you	12/22/2021
ealthine	$\operatorname{ers}\operatorname{DATA}$				Healthineers	have	
	MAN-					deter-	
	AGER					mined	
	v1.1.1 /					that	
	v1.2.1 /					your	
	v1.3.1					Atellica	
						Data	
						Man-	
						ager	
						has a	
						"Java	
						commu-	
						nica-	
						tion	
						engine"	
						service,	
						and	
						you	
						require	
						an	
						imme-	
						diate	
						mitiga-	
						tion,	
						then	
						please	
						contact	
						your	
						Siemens	
						Cus-	
						tomer	
						Care	
						Center	
						or your	
						local	
						Siemens	
						techni-	
						cal	
						support	
						representative.	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
iemens	CENTRAL	INK	Affected	See Notes	Siemens	If you	12/22/2021
ealthineer	rsv16.0.2 /				Healthineers	have	
	v16.0.3					deter-	
						mined	
						that	
						your	
						Cen-	
						traLink	
						has a	
						"Java	
						commu-	
						nica-	
						tion	
						engine"	
						service,	
						and	
						you	
						require	
						a miti-	
						gation,	
						then	
						please	
						contact	
						your	
						Siemens	
						Cus-	
						tomer	
						Care	
						Center	
						or your	
						local	
						Siemens	
						techni-	
						cal	
						support	
						representative.	
liemens	DICOM		Affected	See Notes	Siemens	Workaround:	12/22/2021
[ealthinee]					Healthineers	remove	, ,
	VB10A					the vul-	
						nerable	
						class	
						from	
						the .jar	
						•	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens Healthinee	Somatom rsScope Som5 VC50		Affected	See Notes	Siemens Healthineers	evaluation ongoing	12/22/2021
Siemens Healthinee	Somatom		Affected	See Notes	Siemens Healthineers	evaluation ongoing	12/22/2021
Siemens Healthinee	go.All,		Affected	See Notes	Siemens Healthineers	Workaround: In the mean- time, we recom- mend pre- venting access to port 8090 from other devices by configu- ration of the hospi- tal network.	12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens Healthine	go.Fit, ersSom10 VA30		Affected	See Notes	Siemens Healthineers	Workaround: In the mean- time, we recom- mend pre- venting access to port 8090 from other devices by configu- ration of the hospi- tal	12/22/2021
Siemens Healthine	go.Now, ers Som10 VA10 / VA20 / VA30 / VA40		Affected	See Notes	Siemens Healthineers	network. Workaround: In the mean- time, we recom- mend pre- venting access to port 8090 from other devices by configu- ration of the hospi- tal network.	12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens Healthinee:	go.Open rsPro, Som10 VA30 / VA40		Affected	See Notes	Siemens Healthineers	Workaround: In the mean- time, we recom- mend pre- venting access to port 8090 from other devices by configu- ration of the hospi- tal	12/22/2021
Siemens Healthineer	go.Sim, rsSom10 VA30 / VA40		Affected	See Notes	Siemens Healthineers	network. Workaround: In the mean- time, we recom- mend pre- venting access to port 8090 from other devices by configu- ration of the hospi- tal network.	12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens Healthined	go.Top, ersSom10 VA20 / VA20A_SP5 / VA30 / VA40		Affected	See Notes	Siemens Healthineers	Workaround: In the mean- time, we recom- mend pre- venting access to port 8090 from other devices by configu- ration of the hospi- tal	12/22/2021
Siemens Healthined	go.Up, ersSom10 VA10 / VA20 / VA30 / VA40		Affected	See Notes	Siemens Healthineers	network. Workaround: In the mean- time, we recom- mend pre- venting access to port 8090 from other devices by configu- ration of the hospi- tal network.	12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	MAGNETO	M	Affected	See Notes	Siemens	LOG4J	12/22/2021
Healthine	ersAERA				Healthineers	is used	
	1,5T, MAG-					in the	
	NETOM					context	
	PRISMA,		of the help	of the			
	MAGNE-			help			
	TOM					system.	
	PRISMA					Workaround:	
	FIT, MAG-					close	
	NETOM					port	
	SKYRA 3T					8090	
	NU-					for	
	MARIS/X					stan-	
	VA30A					dalone	
						sys-	
						tems.	
						Setup	
						IP	
						whitelist-	
						ing for	
						"need to	
						access"	
						sys-	
						tems to	
						net-	
						work	
						port	
						8090 in	
						case a	
						second	
						console	
						is	
						connected.	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	Product MAGNETC ers Altea NU- MARIS/X VA20A		Status Affected	Update Available See Notes	Vendor Link Siemens Healthineers	LOG4J is used in the context of the help system. Workaround: close port 8090 for stan- dalone sys- tems. Setup IP whitelist- ing for "need to access" sys- tems to net- work	Last Updated 12/22/2021
						sys- tems to net-	
						console is connected.	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	MAGNETO)M	Affected	See Notes	Siemens	LOG4J	12/22/2021
Healthine	ersALTEA,				Healthineers	is used	
	MAGNE-					in the	
	TOM					context	
	LUMINA,					of the	
	MAGNE-					help	
	TOM					system.	
	SOLA,					Workaround:	
	MAGNE-					close	
	TOM					port	
	VIDA NU-					8090	
	MARIS/X					for	
	VA31A					stan-	
						dalone	
						sys-	
						tems.	
						Setup	
						IP	
						whitelist-	
						ing for	
						"need to	
						access"	
						sys-	
						tems to	
						net-	
						work	
						port	
						8090 in	
						case a	
						second	
						console	
						is	
						connected.	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	MAGNETC ersAmira NU- MARIS/X VA12M		Affected	See Notes	Siemens Healthineers	LOG4J is used in the context of the help system. Workaround: close port	12/22/2021
						8090 for stan- dalone sys- tems. Setup IP whitelist-	
						ing for "need to access" sys-	
						tems to net- work port 8090 in	
						case a second console is connected.	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	MAGNETO	M	Affected	See Notes	Siemens	LOG4J	12/22/2021
Healthinee	rsFree.Max				Healthineers	is used	
	NU-					in the	
	MARIS/X					context	
	VA40					of the	
						help	
						system.	
						Workaround:	
						close	
						port	
						8090	
						for	
						stan-	
						dalone	
						sys-	
						tems.	
						Setup	
						IP	
						whitelist-	
						ing for	
						"need to	
						access"	
						sys-	
						tems to	
						net-	
						work	
						port	
						8090 in	
						case a	
						second	
						console	
						is	
						connected.	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	MAGNETO)M	Affected	See Notes	Siemens	LOG4J	12/22/2021
Healthine	ersSempra				Healthineers	is used	
	NU-					in the	
	MARIS/X					context	
	VA12M					of the	
						help	
						system.	
						Workaround:	
						close	
						port	
						8090	
						for	
						stan-	
						dalone	
						sys-	
						tems.	
						Setup	
						IP	
						whitelist-	
						ing for	
						"need to	
						access"	
						sys-	
						tems to	
						net-	
						work	
						port	
						8090 in	
						case a	
						second	
						console	
						is	
						connected.	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	MAGNETO		Affected	See Notes	Siemens	LOG4J	12/22/2021
Healthine	ersSola fit NU	_			Healthineers	is used	
	MARIS/X					in the	
	VA20A					context	
						of the	
						help	
						system.	
						Workaround:	
						close	
						port	
						8090	
						for	
						stan-	
						dalone	
						sys-	
						tems.	
						Setup	
						IP	
						whitelist-	
						ing for	
						"need to	
						access"	
						sys-	
						tems to	
						net-	
						work	
						port	
						8090 in	
						case a	
						second	
						console	
						is	
						connected.	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens	MAGNETO	M	Affected	See Notes	Siemens	LOG4J	12/22/2021
Healthine	ersSola NU-				Healthineers	is used	
	MARIS/X					in the	
	VA20A					context	
						of the	
						help	
						system.	
						Workaround:	
						close	
						port	
						8090	
						for	
						stan-	
						dalone	
						sys-	
						tems.	
						Setup	
						IP	
						whitelist-	
						ing for	
						"need to	
						access"	
						sys-	
						tems to	
						net-	
						work	
						port	
						8090 in	
						case a	
						second	
						console	
						is	
						connected.	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens Healthine	MAGNETO ersVida NU- MARIS/X VA10A* / VA20A	DM	Affected	See Notes	Siemens Healthineers	LOG4J is used in the context of the help system. Workaround: close port 8090 for stan- dalone sys- tems. Setup IP whitelist- ing for "need to access" sys- tems to net- work port 8090 in case a second console is	12/22/2021
Siemens Healthine	Syngo ers Carbon Space VA10A / VA10A- CUT2 / VA20A		Affected	See Notes	Siemens Healthineers	connected. Workaround: remove the vul- nerable class from the .jar file	12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens Healthine	Syngo Mo- ersbileViewer VA10A		Affected	See Notes	Siemens Healthineers	The vulner- ability will be patch/mitigated in up- coming releases/patches.	12/22/2021
Siemens Healthine	syngo ers Plaza VB20A / VB20A_HF - HF07 / VB30A / VB30A_HF / VB30A_HF / VB30B / VB30C / VB30C_HF - HF06 / VB30C_HF	701 702 701	Affected	See Notes	Siemens Healthineers	Workaround: remove the vul- nerable class from the .jar file	12/22/2021
Siemens Healthine	syngo ersWorkflow MLR VB37A / VB37A_HF / VB37B_HF / VB37B_HF - HF07 / VB37B_HF / VB37B_HF / VB37B_HF	702 701 793 794	Affected	See Notes	Siemens Healthineers	Please contact your Cus- tomer Service to get support on miti- gating the vulnerability.	12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens Healthineer	syngo.via rsVB20A / VB20A_HF0 - HF08 / VB20A_HF9 / VB20B / VB30A / VB30A_HF0)1	Affected	See Notes	Siemens Healthineers	Workarou remove the vul- nerable class from the .jar file	nd:	12/22/2021
	VB30A_HF0 / VB30A_HF9 / VB30B_HF0 / VB40A / VB40A_HF0 - HF02 /VB40B / VB40B_HF0 - HF05 /	01VB30B 01						
	VB50A / VB50A_CU' / VB50A_D4V / VB50B_HF0 - HF03 / VB60A / VB60A_CU'	/B50B 01						
Siemens Healthineer	DMCM / TS / VM / PPWS /	01	Affected	See Notes	Siemens Healthineers	evaluation ongoing	1	12/22/2021
Siemens Healthineer	DS VD12A Cios Select rsFD/I.I. VA21 / VA21-S3P		Affected	See Notes	Siemens Healthineers	evaluation ongoing	1	12/22/2021
Siemens Healthineer	Cios Flow rsS1 / Alpha / Spin VA30		Affected	See Notes	Siemens Healthineers	evaluation ongoing	1	12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Siemens Healthine	syngo.via ersWebViewer VA13B / VA20A / VA20B		Affected	See Notes	Siemens Healthineers	Workaround: remove the vul- nerable class from the .jar file	12/22/2021
Siemens Healthine	X.Ceed ersSomaris 10 VA40*		Affected	See Notes	Siemens Healthineers	Workaround: In the mean- time, we recom- mend pre- venting access to port 8090 from other devices by configu- ration of the hospi- tal network.	12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Siemens	Product X.Cite ersSomaris 10 VA30/VA40	,	Affected	Update Available See Notes	Vendor Link Siemens Healthineers	Notes Workaro In the mean- time, we recommend pre- venting access to port 8090 from other devices by configuration of the	und:	Last Updated 12/22/2021
Sierra Wireless Signald					Sierra Wireless Security Bulletin Signald Gitlab	hospi- tal network.		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
endor ilver eak	Product Orchestrator, Silver Peak GMS		Affected	No No	Vendor Link Security Advisory Notice Apache	Custome managed Orchestrator and legacy GMS products are affected by this vulnerability. This includes onpremise 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		Last Updated 12/14/2021
				494	ı	miti- gate this exploit.		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
SingleWire					SingleWire	This		
					Support Link	advi-		
						sory is		
						avail-		
						able to		
						cus-		
						tomers		
						only		
						and has		
						not		
						been re-		
						viewed		
						by		
1.,					C: C	CISA		
Sitecore					Sitecore Support			
11 -11 1 1					Link			
Skillable SLF4J					Skillable Link SLF4J Link			
SLF 4J Slurm	Slurm	20.11.8	Not		https://slurm.			19/91/9091
num	Siuriii	20.11.0	Affected		schedmd.com/			12/21/2021
			Affected		documentation.			
					html			
SmartBear					SmartBear Link			
SmileCDR					SmileCDR Blog			
mmecDit					Post			
Snakemake	Snakemake	6.12.1	Not		https:			12/21/2021
,1101101110110	21101101110110	0.12.1	Affected		//snakemake.			1-/-1/-0-1
					readthedocs.io/			
					en/stable/			
$5\mathrm{n}0\mathrm{m}$					Sn0m Link			
Snowflake			Not		Snowflake			
			Affected		Community Link			
Snyk	Cloud		Not		Snyk Updates			
	Platform		Affected					
Software					Software AG			
AG								

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes C	ther References	Last Updated
SolarWind	s Database Perfor- mance Analyzer (DPA)	2021.1.x, 2021.3.x, 2022.1.x	Affected	No	Apache Log4j Critical Vulnerability (CVE-2021- 44228) Database Performance Analyzer (DPA) and the Apache Log4j Vulnerability (CVE-2021- 44228)	Workaround avail- able, hotfix under development		12/14/2021
SolarWind	s Server & Applica- tion Monitor (SAM)	SAM 2020.2.6 and later	Affected	No	Apache Log4j Critical Vulnerability (CVE-2021- 44228) Server & Application Monitor (SAM) and the Apache Log4j Vulnerability (CVE-2021-	Workaround avail- able, hotfix under development		12/14/2021
SonarSource Sonatype	ce				44228) SonarSource Sonatype Vulnerability Statement			
SonicWall	Capture Client & Capture Client Portal		Not Affected		Sonic Wall Security Advisory	Log4j2 not used in the Cap- ture Client.		12/12/2021
SonicWall	Access Points		Not Affected		Security Advisory (sonicwall.com)	Log4j2 not used in the Son- icWall Access Points		12/12/2021
SonicWall	Analytics		Under Investigati	on	Security Advisory (sonicwall.com)	Under Review		12/12/2021

Vendor	Product	Version(s) Status	Update Available	Vendor Link	Notes Other Reference	s Last Updated
SonicWall	Analyzer	Under		Security	Under	12/12/2021
		Investiga	tion	Advisory	Review	
				(sonicwall.com)		
SonicWall	Capture	Not		Security	Log4j2	12/12/2021
	Security	Affected		Advisory	not	
	Appliance			(sonicwall.com)	used in	
					the	
					Cap-	
					ture	
					Secu-	
					rity	
					appliance.	
SonicWall	CAS	Under		Security	Under	12/12/2021
		Investiga	tion	Advisory	Review	
				(sonicwall.com)		
SonicWall	Email	Affected	Yes	Security	ES	12/17/2021
	Security			Advisory	10.0.11	
				(sonicwall.com)	and	
					earlier	
					ver-	
					sions	
					are	
					impacted	
SonicWall	Gen5	Not		Security	Log4j2	12/12/2021
	Firewalls	Affected		Advisory	not	
	(EOS)			(sonicwall.com)	used in	
					the	
					appliance.	
SonicWall	Gen6	Not		Security	Log4j2	12/12/2021
	Firewalls	Affected		Advisory	not	
				(sonicwall.com)	used in	
					the	
					appliance.	
SonicWall	Gen7	Not		Security	Log4j2	12/12/2021
	Firewalls	Affected		Advisory	not	
				(sonicwall.com)	used in	
					the	
					appliance.	
SonicWall	GMS	Under		Security	Under	12/12/2021
		Investiga	tion	Advisory	Review	
_				(sonicwall.com)		
SonicWall	MSW	Not		Security	Mysonicwall	12/12/2021
		Affected		Advisory	service	
				(sonicwall.com)	doesn't	
					use	
					Log4j	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
SonicWall	NSM		Not		Security	NSM	12/12/2021
			Affected		Advisory	On-	
					(sonicwall.com)	Prem	
						and	
						SaaS	
						doesn't	
						use a	
						vulner-	
						able	
						version	
SonicWall	SMA 100		Not		Security	Log4j2	12/12/2021
			Affected		Advisory	not	
					(sonicwall.com)	used in	
						the	
						SMA100	
						appliance.	
SonicWall	SMA 1000		Not		Security	Version	12/12/2021
			Affected		Advisory	12.1.0	, ,
					(sonicwall.com)	and	
					,	12.4.1	
						doesn't	
						use a	
						vulner-	
						able	
						version	
SonicWall	SonicCore		Not		Security	SonicCore	12/12/2021
Sollie Wall	2011100010		Affected		Advisory	doesn't	12/12/2021
			1111000004		(sonicwall.com)	use a	
					(some wanteem)	Log4j2	
SonicWall	SonicWall		Not		Security	Log4j2	12/12/2021
Some wan	Switch		Affected		Advisory	not	12/12/2021
	SWITTE		1111000004		(sonicwall.com)	used in	
					(some wanteom)	the	
						Son-	
						icWall	
						Switch.	
SonicWall	WAF		Under		Security	Under	12/12/2021
Some wan	WAL		Investigati	on	Advisory	Review	12/12/2021
			mvestigati	OII		Review	
Conjo Woll	XX/XIX		Not		(sonicwall.com)	Log4;9	19 /19 /9091
SonicWall	VV IN IVI		Not Affected		Security	Log4j2	12/12/2021
			Affected		Advisory	not	
					$({\rm sonic wall.com})$	used in	
						the	
						WNM.	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
SonicWall	WXA		Not Affected		Security Advisory (sonicwall.com)	WXA doesn't use a vulner- able		12/12/2021
Sophos	Cloud Optix		Fixed		Advisory: Log4J zero-day vulnerability AKA Log4Shell (CVE-2021- 44228) Sophos	version Users may have noticed a brief outage around 12:30 GMT as up- dates were de- ployed. There was no evi- dence that the vulner- ability was ex- ploited and to our knowl- edge no cus- tomers are		12/12/2021
Sophos	Reflexion		Not Affected		Advisory: Log4J zero-day vulnerability AKA Log4Shell (CVE-2021- 44228) Sophos	impacted Reflexion does not run an ex- ploitable configura	1	12/12/2021

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

endor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated	
phos	Sophos	< 9.7.2	Affected	No	Advisory: Log4J	The		12/12/2021	
	Mobile				zero-day	Sophos			
	EAS Proxy				vulnerability	Mobile			
					AKA Log4Shell	EAS			
					(CVE-2021-	Proxy,			
					44228) Sophos	run-			
						ning in			
						Traffic			
							Mode, is af-		
						fected.			
						Cus-			
						tomers			
						will			
						need to			
						down-			
						load			
						and			
						install			
						version			
						9.7.2,			
						avail-			
						able			
						from			
						Mon-			
						day			
						Decem-			
						ber 13,			
						2021,			
						on the			
						same			
						ma- chine			
						where			
						it is			
						cur-			
						rently			
						run-			
						ning.			
						Power-			
						Shell			
						mode is			
						not af-			
						fected.			
						Cus-			
						tomers			
						can			
						down-			
						load			
					501	the			
						Stan-			
						dalone			
						EAS			
						Proxy			
						In-			
						staller			
						version			
						9.7.2			
							from the		

the

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Sophos	Sophos ZTNA		Not Affected		Advisory: Log4J zero-day vulnerability AKA Log4Shell (CVE-2021- 44228) Sophos	Sophos ZTNA does not use Log4j.		12/12/2021
SOS					SOS Berlin Link			
Berlin Spambrell	9				Spambrella FAQ			
Spanioren	а				Link			
Spigot					Spigot Security Release			
Splunk	Splunk Add-On for Java Man- agement Extensions App ID 2647	5.2.0 and older	Affected	CVE-2021-44228: 5.2.1 CVE-2021-45046: 5.2.2 CVE-2021-45105: not applicable due to configuration parameters	Splunk Security Advisory for Apache Log4j (CVE-2021- 44228 and CVE-2021- 45046)			9:25 am PT, 12/21/21
Splunk	Splunk Splunk Add-On for JBoss App ID 2954	3.0.0 and older	Affected	CVE-2021-44228: 3.0.1 CVE-2021-45046: 3.0.2 CVE-2021-45105: not applicable due to configuration parameters	Splunk Security Advisory for Apache Log4j (CVE-2021- 44228 and CVE-2021- 45046)			9:25 am PT, 12/21/21
Splunk	Splunk Add-On for Tomcat App ID 2911	3.0.0 and older	Affected	CVE-2021-44228: 3.0.1 CVE-2021-45046: 3.0.2 CVE-2021-45105: not applicable due to configuration parameters	Splunk Security Advisory for Apache Log4j (CVE-2021- 44228 and CVE-2021- 45046)			9:25 am PT, 12/21/21

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Splunk	Data Stream Processor	DSP 1.0.x, DSP 1.1.x, DSP 1.2.x	Affected	Version 1.0.0 and 1.0.1 are out of support and will not receive a patch. Customers on supported versions (> 1.1.0) should patch to the following versions: CVE-2021-44228: 1.2.1-patch02, 1.2.2-patch02 CVE-2021-45046: 1.2.1-patch02, 1.2.2-patch02 CVE-2021-45105: not applicable due to configuration parameters	Splunk Security Advisory for Apache Log4j (CVE-2021- 44228 and CVE-2021- 45046)			9:25 am PT, 12/21/21
Splunk	IT Essentials Work App ID 5403	4.11, 4.10.x (Cloud only), 4.9.x	Affected	CVE-2021-44228: 4.11.1, 4.10.3, 4.9.5 CVE-2021-45046: 4.11.2, 4.10.4, 4.9.6, 4.7.4 CVE-2021-45105: not applicable due to configuration parameters	Splunk Security Advisory for Apache Log4j (CVE-2021- 44228 and CVE-2021- 45046)			9:25 am PT, 12/21/21
Splunk	IT Service Intelligence (ITSI) App ID 1841	4.11.0, 4.10.x (Cloud only), 4.9.x, 4.8.x (Cloud only), 4.7.x, 4.6.x, 4.5.x	Affected	CVE-2021-44228: 4.11.1, 4.10.3, 4.9.5, 4.7.3 CVE-2021-45046: 4.11.2, 4.10.4, 4.9.6, 4.7.4 CVE-2021-45105: not applicable due to configuration parameters	Splunk Security Advisory for Apache Log4j (CVE-2021- 44228 and CVE-2021- 45046)			9:25 am PT, 12/21/21
Splunk	Splunk Connect for Kafka	All versions prior to 2.0.4	Affected	CVE-2021-44228: 2.0.4 CVE-2021-45046: 2.0.5 CVE-2021-45105: 2.0.6	Splunk Security Advisory for Apache Log4j (CVE-2021- 44228 and CVE-2021- 45046)			9:25 am PT, 12/21/21
Splunk	Splunk Enterprise (including instance types like Heavy Forwarders)	All supported non-Windows versions of 8.1.x and 8.2.x only if DFS is used. See Removing Log4j from Splunk Enterprise below for guidance on unsupported versions.	Affected	CVE-2021-44228: 8.1.7.1, 8.2.3.2 CVE-2021-45046: 8.1.7.2, 8.2.3.3 CVE-2021-45105: not applicable due to configuration parameters	Splunk Security Advisory for Apache Log4j (CVE-2021- 44228 and CVE-2021- 45046)			9:25 am PT, 12/21/21

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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-2021-44338: 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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
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
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 Infrastruc- ture 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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Splunk Sprecher Automatio	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) Sprecher Automation			9:25 am PT, 12/21/21
С .	О .		TT 1		Security Alert	С .		
Spring	Spring Boot		Unknown		https://spring. io/blog/2021/12/ 10/log4j2- vulnerability- and-spring-boot	Spring Boot users are only af- fected by this vulner- ability if they have switched the default logging system to		
Spring Boot					Spring Boot Vulnerability	Log4J2		
StarDog					Statement StarDog			
STERIS	Advantage		Not		STERIS			12/22/2021
STERIS	Advantage Plus		Affected Not Affected		Advisory Link STERIS Advisory Link			12/22/2021
STERIS	DSD Edge		Not		STERIS			12/22/2021
STERIS	EndoDry		Affected Not		Advisory Link STERIS			12/22/2021
STERIS	RapidAER		Affected Not		Advisory Link STERIS			12/22/2021
STERIS	Endora		Affected Not		Advisory Link STERIS			12/22/2021
STERIS	Canexis 1.0		Affected Not Affected		Advisory Link STERIS Advisory Link			12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
STERIS	ConnectoHIS	S	Not		STERIS			12/22/2021
			Affected		Advisory Link			
STERIS	ScopeBuddy	r+	Not		STERIS			12/22/2021
			Affected		Advisory Link			
STERIS	DSD-201,		Not		STERIS			12/22/2021
	,		Affected		Advisory Link			1 1
STERIS	CER		Not		STERIS			12/22/2021
.5	Optima		Affected		Advisory Link			//
STERIS	Renatron		Not		STERIS			12/22/2021
SILIUS	recirculon		Affected		Advisory Link			12/22/2021
STERIS	ConnectAssı	uro	Not		STERIS			12/22/2021
STER	Technology	uic	Affected		Advisory Link			12/22/2021
STERIS	SPM		Not		STERIS			12/22/2021
STERIS			Affected		Advisory Link			12/22/2021
	Surgical		Affected		Advisory Link			
	Asset							
	Tracking							
CERTIFIC	Software		NT /		CERTIFIC			10/00/0001
STERIS	CS-iQ		Not		STERIS			12/22/2021
	Sterile		Affected		Advisory Link			
	Processing							
~	Workflow							
STERIS	AMSCO		Not		STERIS			12/22/2021
	2000		Affected		Advisory Link			
	SERIES							
	WASHER							
	DISINFECT	TORS						
STERIS	AMSCO		Not		STERIS			12/22/2021
	3000		Affected		Advisory Link			
	SERIES							
	WASHER							
	DISINFECT	TORS						
STERIS	AMSCO		Not		STERIS			12/22/2021
	5000		Affected		Advisory Link			, ,
	SERIES							
	WASHER							
	DISINFECT	TORS						
STERIS	AMSCO		Not		STERIS			12/22/2021
	7000		Affected		Advisory Link			7 7 -
	SERIES							
	WASHER							
	DISINFECT	TORS						
STERIS	RELIANCE		Not		STERIS			12/22/2021
SILLIUS	444		Affected		Advisory Link			12/22/2021
	WASHER		meeted		Tidvisory Link			
	DISINFECT	TOR						
	DISTALECT	on						

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
STERIS	RELIANCE SYNERGY WASHER DISINFECTOI	R	Not Affected		STERIS Advisory Link			12/22/2021
STERIS	RELIANCE VISION 1300 SERIES CART AND UTENSIL WASHER DISINFECTOI		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	RELIANCE VISION MULTI- CHAM- BER WASHER DISINFECTOI	R	Not Affected		STERIS Advisory Link			12/22/2021
STERIS	RELIANCE VISION SINGLE CHAM- BER WASHER DISINFECTOI		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	AMSCO 400 MEDIUM STEAM STERILIZER		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	AMSCO 400 SMALL STEAM STERILIZERS	3	Not Affected		STERIS Advisory Link			12/22/2021
STERIS	AMSCO 600 MEDIUM STEAM STERILIZER		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	AMSCO CENTURY MEDIUM STEAM STERILIZER		Not Affected		STERIS Advisory Link			12/22/2021

Vendor	Product Version(s)	Status Update Available	Vendor Link Notes Other References	Last Updated
STERIS	AMSCO CENTURY SMALL STEAM STERILIZER	Not Affected	STERIS Advisory Link	12/22/2021
STERIS	AMSCO EAGLE 3000 SERIES STAGE 3 STEAM	Not Affected	STERIS Advisory Link	12/22/2021
STERIS	STERILIZERS AMSCO EVOLU- TION FLOOR LOADER STEAM STERILIZER	Not Affected	STERIS Advisory Link	12/22/2021
STERIS	AMSCO EVOLU- TION MEDIUM STEAM STERILIZER	Not Affected	STERIS Advisory Link	12/22/2021
STERIS	CELERITY HP INCUBATOR	Not Affected	STERIS Advisory Link	12/22/2021
STERIS	CELERITY STEAM INCUBATOR	Not Affected	STERIS Advisory Link	12/22/2021
STERIS	VERIFY INCUBA- TOR FOR ASSERT SELF- CONTAINED BIOLOGI- CAL INDICATORS	Not Affected	STERIS Advisory Link	12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
STERIS	SYSTEM 1 endo LIQUID CHEMI- CAL STERI- LANT PROCESS- ING SYSTEM		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	V-PRO 1 LOW TEMPER- ATURE STERIL- IZATION SYSTEM		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	V-PRO 1 PLUS LOW TEMPER- ATURE STERIL- IZATION SYSTEM		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	V-PRO MAX 2 LOW TEMPER- ATURE STERIL- IZATION SYSTEM		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	V-PRO MAX LOW TEMPER- ATURE STERIL- IZATION SYSTEM		Not Affected		STERIS Advisory Link			12/22/2021
STERIS	V-PRO S2 LOW TEMPER- ATURE STERIL- IZATION SYSTEM		Not Affected		STERIS Advisory Link			12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
STERIS	SecureCare		Not		STERIS			12/22/2021
	ProCon-		Affected		Advisory Link			
	nect							
	Technical							
	Support							
	Services							
STERIS	HexaVue		Not		STERIS			12/22/2021
	Integration		Affected		Advisory Link			
	System							
STERIS	IDSS		Not		STERIS			12/22/2021
	Integration		Affected		Advisory Link			
	System							
STERIS	Harmony		Not		STERIS			12/22/2021
	iQ		Affected		Advisory Link			
	Integration							
	Systems							
STERIS	HexaVue		Not		STERIS			12/22/2021
			Affected		Advisory Link			
STERIS	Connect		Not		STERIS			12/22/2021
	Software		Affected		Advisory Link			
STERIS	Harmony		Not		STERIS			12/22/2021
	iQ Perspec-		Affected		Advisory Link			
	tives Image							
	Manage-							
	ment							
	System							
STERIS	Clarity		Not		STERIS			12/22/2021
	Software		Affected		Advisory Link			
STERIS	Situational		Not		STERIS			12/22/2021
	Awareness		Affected		Advisory Link			
	for							
	Everyone							
	Display							
	(S.A.F.E.)							
STERIS	RealView		Not		STERIS			12/22/2021
	Visual		Affected		Advisory Link			
	Workflow							
	Manage-							
	ment							
	System							
STERIS	ReadyTracke	r	Not		STERIS			12/22/2021
			Affected		Advisory Link			
Sterling					IBM Statement			
Order								
TDAG								
IBM								

StormShield StormShield StrangeBee StrangeBee Thellive Statement & Cortex Tratodesk Stratodesk Stratement Strimzi Strimzi Stripe Stripe Support Styra Styra Security Notice Sumologic Sumologic Sumologic Superna Sumologic Styrea Sumologic Superna EYEGLASS Technical Advisory Suprema Suprema SUSE Suprema SUSE Suprema Suyeren Suprema Suyeren Suprema Suyeren Suprema Suyeren Suprema Sweepwidget Suprema Sweepwidget Suprema Sweepwidget Suprema Sweepwidget Suprema Sweepwidget Suprema Sweepwidget Suprema Synchro MSP Advisory Synclogy	pdated
StrangeBee Statement TheHilve Statement Stratodosk Stratodes Strinzi Strimzi Stripe Stripe Support Stya Stripe Support Stya Stripe Support Stya Stripe Support Sumologic Statement Sumologic Statement Sumologic Statement Superna Superna EYEGLASS EYEGLASS Superna EYEGLASS Suprema EYEGLASS Superna Superna Inc SUSE Suprema Inc Superna Inc SUSE Statement Sweepwidget Succeptified Swepwidget Succeptified Synchro Synchro MSP MSP Advisory Synchro Synchro Synchro Synchro Synopsys Advisory Syntero Syntero Syntero Syntero Syntero <td< td=""><td></td></td<>	
Thellive Statement & Cortex Stratodesk STratodesk Strimzi Statement Stripe Stripe Support Strya Strya Security Notice Notice Sumologic Statement Sumologic Statement Superna Superna EYEGLASS EYEGLASS Suprema EYEGLASS Suprema Suprema Inc Inc Suprema Inc Sweepwidget Suepwidget Sweepwidget Statement Sweepwidget Statement Swyx Synchro MSP MSP Advisory Synchro Synchro MSP MSP Advisory Synology Advisory <td></td>	
& Cortex Stratodesk STratodesk Strimzi Statement Stripe Stripe Support Styn Styra Security Notice Notice Sumologic Sumologic Superna Sumologic Superna Superna EYEGLASS EYEGLASS Suprema Suprema Inc Technical Juc Advisory Superna Inc Suprema Inc Inc Suprema Inc Sweepwidget Sweepwidget Sweepwidget Sweepwidget Swyx Swyx Advisory Synchro Synchro MSP MSP Advisory Synclify Advisory Synology Advisory Synology Advisory Synopsys Advisory Syntevo Syntevo Syntevo Syntevo Syntevo Syntevo Syntevo Statement Statement Statement <td></td>	
Stratodesk STratodesk Strimzi Statement Stripe Strip Support Styra Strip Support Styra Security Notice Sumologic Statement SumoLogic Statement Superna Superna EYEGLASS EYEGLASS Technical Advisory Superna Superna Inc Inc SUSE Statement Sweepwidget Succepwidget Sweepwidget Statement Swyx Synchro MSP MSP Advisory Synchro Synchro MSP MSP Advisory Synology Advisory Synology Advisory Synopsys Advisory Synopsys Synopsys Syntevo Syntevo Systid Https://www.	
Strimzi Statement Stripe Stripe Support Styra Stripe Support Styra Sceurity Notice Sumologic Sumologic SumoLogic Statement Superna Superna EYEGLASS EYEGLASS EYEGLASS EYEGLASS Superma Superma Inc Inc Superma Inc SuS Superma Inc SuS Superma Inc Sweepwidget Superma Inc Sweepwidget Superma Inc Sweepwidget Superma Sweepwidget Synchro Swyx Synchro Synchro Synchro <td></td>	
Strimzi Striment Stripe Stripe Support Styra Styra Security Nucice Sumologic Sumologic Sumologic Sumologic Statement Superna Release Notes Superna Superna EYEGLASS Technical Advisory Advisory Suprema Suprema Inc Inc Suprema Inc Suy Supermind Inc Sweepwidget Succepwidget Sweepwidget Sveepwidget Swyx Synchro MSP Synchro Synchro MSP MSP Synchro MSP MSP Synchro MSP Synclify Advisory Synclogy Advisory Synopsys Advisory Synopsys Advisory Syntevo Syntevo Syntevo Synternet Syntei Syntement Syntevo Syntevo Syntei Syntevo	
Stripe Stripe Support Styra Styra Security Notice Notice Sumologie Sumologie SumoLogic Sumologie Superna Release Notes Superna Superna EYEGLASS EYEGLASS Technical Advisory Superna Inc Superma Inc Inc Susepwidget Sweepwidget Suetement Sweyx Sweepwidget Swepwidget Swepwidget Synchro Synchro MSP MSP Advisory Synchro Synchro MSP MSP Advisory Synology	
Stripe Stripe Support Styra Styra Security Sumologic Sumologic Sumologic Statement Sumologic Release Notes Superna Superna EYEGLASS Technical Advisory Technical Suprema Suprema Inc Inc SUSE Statement Sweepwidget Sweepwidget Sweepwidget Statement Swyx Sweepwidget Synchro Synchro MSP MSP Advisory Syncplify Advisory Syncplify Advisory Synology Advisory Synolog	
Styra Styra Security Sumologic Sumologic SumoLogic Sumologic Release Notes Release Notes Superna Superna EYEGLASS EYEGLASS Technical Advisory Superma Inc Superma Inc Inc SUSE Sweepwidget Sweepwidget Swyx Sweepwidget Synchro Suprema MSP Advisory Synchro MSP Advisory Syncplify Advisory Synology Advisory Synology Advisory Synopsys Advisory Synopsys Synopsys Syntevo Syntevo SysAid Statement StysAid https://www.	
Sumologic Notice Sumologic Statement Sumologic Sumologic Superna Superna EYEGLASS EYEGLASS Technical Advisory Superma Superma Inc Ine SUSE Statement Sweepwidget Sweepwidget Swyx Sweepwidget Swyx Sweepwidget Synchro Synchro MSP MSP Advisory Syncplify Advisory Syncplify Synclify Synology Advisory Synology Synology Synopsys Advisory Synopsys Advisory Syntevo Syntevo SysAid Inttps://www.	
Sumologic Sumologic SumoLogic Release Notes Superna Superna EYEGLASS EYEGLASS Technical Advisory Suprema Inc Inc SUSE Statement Sweepwidget Suse Statement Swyx Sweepwidget Swyx Swyx Advisory Synchro Synchro MSP MSP Advisory Syncplify Advisory Synclogy Synclylify Advisory Synology Synopsys Synopsys Syntevo Syntevo SysAid https://www.	
SumoLogie Statement Superna Kelease Notes Superna Superna EYEGLASS EYEGLASS Technical Advisory Suprema Suprema Inc Inc Surrema Inc SuSE Susepwidget Sweepwidget Sweepwidget Swyx Swyx Advisory Synchro Synchro MSP MSP Advisory Syncplify Advisory Syncplify Advisory Synology Synology Synopsys Advisory Synopsys Advisory Syntevo Syntevo SysAid Statement	
SumoLogic Sumologic Release Notes Superna Superna EYEGLASS EYEGLASS Technical Advisory Suprema Suprema Inc Ine Suse Statement Sweepwidget Sweepwidget Swyx Sweepwidget Swyx Swyx Advisory Synchro Synchro MSP MSP Syncplify Syncplify Advisory Synology Advisory Synology Advisory Synopsys Advisory Synopsys Advisory Syntevo Syntevo SysAid https://www.	
Superna Release Notes Superna Superna EYEGLASS Technical Advisory Advisory Suprema Inc Inc Inc SUSE Statement Sweepwidget Sweepwidget Swyx Sweepwidget Swyx Swyx Advisory Synchro Synchro MSP MSP Advisory Syncplify Syncplify Advisory Synology Synology Advisory Synopsys Advisory Synopsys Synopsys Advisory Synopsys Syntevo Syntevo SysAid https://www.	
Superna Superna EYEGLASS EYEGLAS Technical Advisory Suprema Suprema Inc Inc Inc SUSE SUSE Statement Sweepwidget Sweepwidget Swyx Swyx Advisory Synchro Synchro MSP MSP Advisory Syncplify Syncplify Synology Synology Synology Synology Synopsys Advisory Synopsys Advisory Syntevo Synopsys Syntevo Syntevo SysAid https://www.	
EYEGLASS Technical Advisory Suprema Suprema Inc Inc SUSE SUSE SUSE Statement Sweepwidget Statement Swyx Swyx Advisory Synchro Synchro MSP MSP Advisory Syncplify Advisory Synclify Advisory Synology Synology Advisory Synopsys Syntevo Syntevo Syntevo Statement SysAid https://www.	
EYEGLASS Technical Advisory Suprema Suprema Inc Inc SUSE SUSE SUSE Statement Sweepwidget Statement Swyx Swyx Advisory Synchro Synchro MSP MSP Advisory Syncplify Advisory Synclify Advisory Synology Synology Advisory Synopsys Syntevo Syntevo Syntevo Statement SysAid https://www.	
Suprema Technical Advisory Suprema Inc Inc SUSE SUSE Statement Sweepwidget Sweepwidget Swyx Swyx Advisory Synchro Synchro MSP MSP Advisory Syncplify Syncplify Advisory Synology Synology Advisory Synopsys Synopsys Syntevo Syntevo SysAid https://www.	
Suprema Advisory Suprema Inc Inc SUSE SUSE Statement Sweepwidget Sweepwidget Swyx Statement Swyx Synchro Synchro Synchro MSP MSP Advisory Synclify Advisory Synology Synology Synopsys Advisory Synopsys Synopsys Syntevo Syntevo SysAid https://www.	
Suprema Suprema Inc SUSE SUSE Statement Sweepwidget Sweepwidget Swyx Statement Swyx Swyx Advisory Synchro Synchro MSP MSP Advisory Syncplify Advisory Synology Synology Synology Advisory Synopsys Advisory Syntevo Syntevo Syntevo Syntevo SysAid https://www.	
Inc SUSE SUSE Statement Sweepwidget Sweepwidget Swyx Statement Synchro Synchro MSP MSP Advisory Syncplify Syncplify Synology Synology Synology Synology Synopsys Synopsys Syntevo Syntevo SysAid https://www.	
SUSESUSE StatementSweepwidgetStatementSwyxSwyx AdvisorySynchroSynchro MSPMSPAdvisorySyncplifySyncplifySynologySynologySynologySynologySynopsysAdvisorySynopsysSynopsysSyntevoSyntevoSysAidhttps://www.	
Sweepwidget Sweepwidget Swyx Statement Synchro Synchro MSP MSP Advisory Syncplify Syncplify Synology Advisory Synopsys Synopsys Synopsys Synopsys Syntevo Syntevo SysAid https://www.	
Swyx Statement Synchro Synchro MSP MSP Advisory Syncplify Syncplify Synology Advisory Synopsys Synopsys Syntevo Syntevo SysAid https://www.	
Swyx Synchro Synchro MSP MSP Syncplify Syncplify Advisory Synology Synology Synology Synopsys Synopsys Synopsys Synopsys Syntevo Syntevo Syntevo Synopsys Syntevo Statement SysAid Swyx Advisory Synchro MSP Advisory Syncplify Advisory Synology Advisory Synopsys Advisory Syntevo Statement https://www.	
Synchro MSP Advisory Syncplify Synclogy Synology Synology Synology Synopsys Advisory Synopsys Synopsys Synopsys Advisory Synopsys Synopsys Advisory Synopsys Advisory Syntevo Syntevo Syntevo Statement SysAid	
MSP Syncplify Syncplify Synclogy Synology Synology Synology Synology Synology Synopsys Synopsys Synopsys Synopsys Synopsys Synopsys Syntevo Syntevo Syntevo Statement SysAid https://www.	
Syncplify Syncplify Advisory Synology Synology Advisory Synopsys Synopsys Advisory Syntevo Syntevo Syntevo Syntevo Statement SysAid Syncplify Advisory Synology Advisory Synopsys Advisory Syntevo Statement https://www.	
Synology Synology Synology Advisory Synopsys Synopsys Advisory Syntevo Syntevo Syntevo Syntevo Syntevo Statement SysAid https://www.	
Synology Synology Advisory Synopsys Synopsys Advisory Syntevo Syntevo Syntevo Syntevo Statement SysAid https://www.	
Synopsys Synopsys Syntevo Syntevo SysAid Advisory Syntevo Syntevo Statement https://www.	
Synopsys Syntevo Syntevo SysAid Synopsys Advisory Syntevo Statement https://www.	
Syntevo Syntevo SysAid Advisory Syntevo Statement https://www.	
Syntevo SysAid Syntevo Statement https://www.	
Statement SysAid https://www.	
SysAid https://www.	
evenid com /ln/	
sysaid.com/lp/ important-	
update-	
regarding-	
apache-log4j	
Sysdig https://sysdig.	
com/blog/cve-	
critical-	
vulnerability-	
$\log 4\mathrm{j}/$	

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Tableau	Tableau Server	The following versions and lower: 2021.4, 2021.3.4, 2021.2.5, 2021.1.8, 2020.4.11, 2020.3.14, 2020.2.19, 2020.1.22, 2019.4.25, 2019.3.26, 2019.2.29, 2019.1.29, 2018.3.29	Affected	Yes	Apache Log4j2 vulnerability (Log4shell)			12/22/2021
Tableau	Tableau Desktop	The following versions and lower: 2021.4, 2021.3.4, 2021.2.5, 2021.1.8, 2020.4.11, 2020.3.14, 2020.2.19, 2020.1.22, 2019.4.25, 2019.3.26, 2019.2.29, 2019.1.29, 2018.3.29	Affected	Yes	Apache Log4j2 vulnerability (Log4shell)			12/22/2021
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, 2019.4.2, 2	Affected	Yes	Apache Log4j2 vulnerability (Log4shell)			12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Γableau	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		Yes	Apache Log4j2 vulnerability (Log4shell)			12/22/2021
Talend					https://jira. talendforge.org/ browse/TCOMP- 2054			
Tanium	All	All versions	Not Affected		Tanium Statement	Tanium does not use Log4j.		12/21/2021
ealiumIQ	, wordManager				TealiumIQ Security Update TeamPasswordMa			
Ceamviewe					Blog TeamViewer Bulletin	nager		
Tech Software	OneAegis (f/k/a IRBManager	All versions	Not Affected		Log4j CVE-2021-44228 Vulnerability Impact Statement	OneAeg does not use Log4j.	is	12/15/2021
Fech Software	SMART	All versions	Not Affected		Log4j CVE-2021-44228 Vulnerability Impact Statement	SMART does not use Log4j.		12/15/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Tech Software	Study Binders	All versions	Not Affected		Log4j CVE-2021-44228 Vulnerability Impact Statement	Study Binders does not use Log4j.		12/15/2021
TechSmith					TechSmith Article	Log4J.		
Telestream	l				Telestream Bulletin			
Tenable	Tenable.io / Nessus		Not Affected		Tenable log4j Statement	None of Tenable's products are running the version of Log4j vulnerable to CVE-2021-44228 or CVE-2021-45046 at this		
Thales	CipherTrust Applica- tion Data Protection (CADP) – CAPI.net & Net Core		Not Affected		Thales Support	time		12/17/2021
Thales	CipherTrust Cloud Key Manager (CCKM) Embedded		Not Affected		Thales Support			12/17/2021
Thales	CipherTrust Database Protection		Not Affected		Thales Support			12/17/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Thales	CipherTrust Manager		Not Affected		Thales Support			12/17/2021
Thales	CipherTrust Transparent Encryption (CTE/VTE/ U)	СТЕ-	Not Affected		Thales Support			12/17/2021
Thales	CipherTrust Vaultless Tokeniza- tion (CTS, CT-VL)		Not Affected		Thales Support			12/17/2021
Thales	Data Protection on Demand		Not Affected		Thales Support			12/17/2021
Thales	Data Security Manager (DSM)		Not Affected		Thales Support			12/17/2021
Thales	KeySecure		Not Affected		Thales Support			12/17/2021
Thales	Luna EFT		Not Affected		Thales Support			12/17/2021
Thales	Luna Network, PCIe, Luna USB HSM and backup devices		Not Affected		Thales Support			12/17/2021
Thales	Luna SP		Not Affected		Thales Support			12/17/2021
Thales	ProtectServe HSMs	r	Not Affected		Thales Support			12/17/2021
Thales	SafeNet Authentica- tion 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 ID- Prime(all products)		Not Affected		Thales Support			12/17/2021

Vendor	Product	Version(s) Status	Update Available	Vendor Link	Notes Other Re	eferences Last Updated
Thales	SafeNet	Not		Thales Support		12/17/2021
	LUKS	Affected	l			
Thales	SafeNet	Not		Thales Support		12/17/2021
	Protec-	Affected	1			
	tApp(PA)					
	CAPI, .Net					
	& Net Core					
Thales	SafeNet	Not		Thales Support		12/17/2021
	ProtectDB	Affected	1			
TD1 1	(PDB)	NT .		TPI 1 C		10/17/2001
Thales	SafeNet	Not	1	Thales Support		12/17/2021
TP11	ProtectV	Affected	1	TT11 C		19/17/9091
Thales	Safenet ProtectFile	Not Affected	1	Thales Support		12/17/2021
	and	Affected	1			
	ProtectFile-					
	1 Totaccor ne					
	Fuse					
Thales	SafeNet	Not		Thales Support		12/17/2021
	Transform	Affected	l			
	Utility					
	(TU)					10/17/1001
Thales	SafeNet	Not		Thales Support		12/17/2021
	Trusted	Affected	1			
	Access					
TP1 1	(STA)	Not		TT11 C		19/17/9091
Thales	SafeNet	Affected	1	Thales Support		12/17/2021
	PKCS#11 and TDE	Апестес	1			
Thales	SafeNet	Not		Thales Support		12/17/2021
Thates	SQL EKM	Affected	1	Thales Support		12/11/2021
Thales	SAS on	Not	1	Thales Support		12/17/2021
1116165	Prem	Affected	1	Thates support		12/11/2021
	(SPE/PCE)	711100000	•			
Thales	Sentinel	Not		Thales Support		12/17/2021
	EMS	Affected	l	~ «FF		/ /
	Enterprise					
	OnPremise					
Thales	Sentinel	Not		Thales Support		12/17/2021
	ESDaaS	Affected	l	11		, ,
Thales	Sentinel Up	Not		Thales Support		12/17/2021
	•	Affected	l	**		, ,
Thales	Sentinel	Not		Thales Support		12/17/2021
	RMS	Affected	l			
Thales	Sentinel	Not		Thales Support		12/17/2021
	Connect	Affected	l			

Vendor	Product Version	(s) Status Update Available	Vendor Link Notes Other References	Last Updated
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 Applica- tion 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 Tokeniza- tion 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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Thales	CipherTrust Batch Data Transfor- mation (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 To- kenization (CT-V) / SafeNet To- kenization Manager		Affected		Thales Support			12/17/2021
Thales	CipherTrust/ PDBCTL	/SafeNet	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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Thales	Sentinel Profes-		Affected		Thales Support			12/17/2021
	sional							
	Services							
	compo-							
	nents (both Thales							
	hosted &							
	hosted on-							
	premises by							
	customers)							
Thales	Sentinel SCL		Affected		Thales Support			12/17/2021
Thales	Thales		Affected		Thales Support			12/17/2021
	Data							
	Platform							
(TD)	(TDP)(DDC		Not		Thermo-Calc	Use the		10/00/0001
Thermo-Calc	Thermo- Calc	2022a	Affected		Advisory Link	pro-		12/22/2021
Carc	Carc		Affected		Advisory Link	gram		
						as		
						normal,		
						Install		
						the		
						2022a		
						patch when		
						available	e	
Thermo-	Thermo-	2021b	Not		Thermo-Calc	Use the		12/22/2021
Calc	Calc		Affected		Advisory Link	pro-		. ,
						gram		
						as		
						normal		

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Thermo-Calc	Thermo-Calc	2018b to 2021a	Not Affected		Thermo-Calc Advisory Link	Use the program as normal, delete the Log4j 2 files in the program installation if required, see advisory for		12/22/2021
Thermo-Calc	Thermo-Calc	2018a and earlier	Not Affected		Thermo-Calc Advisory Link	instructio Use the pro- gram as normal	ns.	12/22/2021
Thermo Fisher Scientific			Unknown		Thermo Fisher Scientific Advisory Link	210111101		12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Thomson	HighQ Appliance	<3.5	Affected	Yes	https: //highqsolutions. zendesk.com	Reported by vendor - Documentation is in vendor's client portal (login required). This advisory is available to customer only and has not been reviewed by		12/20/2021
ThreatLocke	er				ThreatLocker	CISA.		
ThycoticCen	n Seify et Server	N/A	Not Affected		Log4j Statement ThycoticCentrify Products NOT Affected by CVE-2021-44228			12/10/15
ThycoticCen	n Frify ilege Manager	N/A	Not Affected		Exploit ThycoticCentrify Products NOT Affected by CVE-2021-44228 Exploit			12/10/15
	n Aify ount Lifecycle Manager	N/A	Not Affected		ThycoticCentrify Products NOT Affected by CVE-2021-44228 Exploit			12/10/15

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
ThycoticC	en Frif yileged Behavior Analytics	N/A	Not Affected		ThycoticCentrify Products NOT Affected by CVE-2021-44228 Exploit			12/10/15
ThycoticC	en Dify Ops Secrets Vault	N/A	Not Affected		ThycoticCentrify Products NOT Affected by CVE-2021-44228 Exploit			12/10/15
ThycoticC	en Gify nection Manager	N/A	Not Affected		ThycoticCentrify Products NOT Affected by CVE-2021-44228 Exploit			12/10/15
ThycoticC	en Prif sword Reset Server	N/A	Not Affected		ThycoticCentrify Products NOT Affected by CVE-2021-44228 Exploit			12/10/15
ThycoticC	en Glón d Suite	N/A	Not Affected		ThycoticCentrify Products NOT Affected by CVE-2021-44228 Exploit			12/10/15
Tibco Top Gun Technology					Tibco Support Link TGT Bulletin			
(TGT) TopDesk Topicus Security Topix Tosibox	Topicus KeyHub	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(al	l)Affected	Yes	Statement on Apache Log4j Vulnerability	Update is Beta. Reddit: over-written vulner-able log4j with 2.15 files as potential workarou Though that should now be done with 2.16	Tp Community Link,Reddit Link	12/15/2021
TrendMicro Tricentis Tosca	o All		Under Investigation	on	https://success. trendmicro.com/ solution/ 000289940 Tricentis Tosca Statement			
Tripwire					Tripwire Log4j Statement			
Trimble	eCognition	10.2.0 Build 4618	Affected	No	Details are shared with active subscribers	Remedia steps pro- vided by Trimble	tion	12/23/2021
${\bf TrueNAS}$					TrueNAS	Timioic		
Tufin TYPO3					Statement Tufin Statement TYPO3 Statement			
Ubiquiti	UniFi Network Application	6.5.53 & lower versions	Affected	Yes	UniFi Network Application 6.5.54 Ubiquiti Community			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Ubiquiti	UniFi Network Controller	6.5.54 & lower versions	Affected	Yes	UniFi Network Application 6.5.55 Ubiquiti Community		6.5.54 is reported to still be vulnerable. 6.5.55 is the new recommendation for mitigatin log4j vulnerabilities by updating to log4j 2.16.0	12/15/2021
Ubuntu					Ubuntu Security			
Umbraco					Advisory Umbraco Security			
UniFlow					Advisory UniFlow Security Advisory			
Unify					Unify ATOS			
ATOS					Advisory			
Unimus					Unimus Statement			
USSIGNAI					USSIGNAL MSP			
MSP					Statement			
VArmour					VArmour			
Vanion	A	All	Under		Statement Varian Advisory			10 /00 /0001
Varian	Acuity	All	Investigation	on	Varian Advisory Link			12/22/2021
Varian	DITC	All	Under		Varian Advisory			12/22/2021
			Investigation	on	Link			
Varian	ARIA	All	Not		Varian Advisory			12/22/2021
	Connect (Cloverleaf)		Affected		Link			
Varian	(Cloverlear) ARIA	All	Not		Varian Advisory			12/22/2021
Verien	oncology informa-		Affected		Link			12/22/2021
	tion system for Medical Oncology							
Varian	XMediusFax	All	Under		Varian Advisory			12/22/2021
	for ARIA		Investigation	on	Link			
	oncology informa-							
	tion system							
	for Medical							
	Oncology							
Varian	ARIA	All	Not		Varian Advisory			12/22/2021
	oncology in- formation		Affected		Link			
	system for							
	Radiation							
	Oncology							

Vendor	Product	Version(s)	Status Update Available	Vendor Link Notes Other References	Last Updated
Varian	ARIA	All	Not	Varian Advisory	12/22/2021
	eDOC		Affected	Link	
Varian	XMediusFax	All	Under	Varian Advisory	12/22/2021
	for ARIA		Investigation	Link	
	oncology in-				
	formation				
	system for				
	Radiation				
	Oncology				
Varian	ARIA	All	Not	Varian Advisory	12/22/2021
	Radiation		Affected	Link	
	Therapy				
	Manage-				
	ment				
	System				
	(RTM)				
Varian	Bravos	All	Not	Varian Advisory	12/22/2021
	Console		Affected	Link	
Varian	Clinac	All	Under	Varian Advisory	12/22/2021
			Investigation	Link	
Varian	Cloud	All	Not	Varian Advisory	12/22/2021
	Planner		Affected	Link	
Varian	DoseLab	All	Not	Varian Advisory	12/22/2021
			Affected	Link	
Varian	Eclipse	All	Not	Varian Advisory	12/22/2021
	treatment		Affected	Link	
	planning				
	software				
Varian	ePeerReview	All	Under	Varian Advisory	12/22/2021
			Investigation	Link	
Varian	Ethos	All	Not	Varian Advisory	12/22/2021
			Affected	Link	
Varian	FullScale	All	Under	Varian Advisory	12/22/2021
	oncology		Investigation	Link	
	IT				
	solutions				
Varian	Halcyon	All	Under	Varian Advisory	12/22/2021
	system		Investigation	Link	
Varian	Identify	All	Not	Varian Advisory	12/22/2021
			Affected	Link	
Varian	Information	All	Not	Varian Advisory	12/22/2021
	Exchange		Affected	Link	
	Manager				
	(IEM)				
Varian	InSightive	All	Under	Varian Advisory	12/22/2021
	Analytics		Investigation	Link	•

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
Varian	Large Integrated Oncology Network (LION)	All	Not Affected		Varian Advisory Link		12/22/2021
Varian	ICAP '	All	Not Affected		Varian Advisory Link		12/22/2021
Varian	Mobius3D platform	All	Not Affected		Varian Advisory Link		12/22/2021
Varian	ProBeam	All	Not Affected		Varian Advisory Link		12/22/2021
Varian	Qumulate	All	Not Affected		Varian Advisory Link		12/22/2021
Varian	Real-time Position Manage- ment (RPM)	All	Not Affected		Varian Advisory Link		12/22/2021
Varian	Respiratory Gating for Scanners (RGSC)	All	Not Affected		Varian Advisory Link		12/22/2021
Varian	SmartConne solution	ectAll	Affected		Varian Advisory Link	See Knowl- edge Article: 000038850 on MyVarian	12/22/2021
Varian	SmartConne solution Policy Server	ect All	Affected		Varian Advisory Link	See Knowl- edge Arti- cles: 000038831 and 000038832 on MyVarian	12/22/2021
Varian	PaaS	All	Not Affected		Varian Advisory Link	wy varian	12/22/2021
Varian	TrueBeam radiother-apy	All	Not Affected		Varian Advisory Link		12/22/2021
Varian	system UNIQUE system	All	Under Investigation	on	Varian Advisory Link		12/22/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Varian	Varian Authentication and Identity Server (VAIS)	All	Not Affected		Varian Advisory Link			12/22/2021
Varian	Varian Managed Services Cloud	All	Under Investigation	on	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 radiother- apy system	All	Not Affected		Varian Advisory Link			12/22/2021
Varian Varnish Software Varonis Veeam Venafi Veritas NetBackup Vertica Viso Trust		All	Not Affected		Varian Advisory Link Varnish Software Security Notice Varonis Notice Veeam Statement Venafi Statement Verita Statement Vertica Statement Viso Trust Statement			12/22/2021
VMware	API Portal for VMware Tanzu	1.x	Affected	No	VMSA-2021- 0028.1 (vmware.com)			12/12/2021
VMware	App Metrics	2.x	Affected	Yes	VMSA-2021- 0028.1 (vmware.com)			12/12/2021
VMware	Healthwatch for Tanzu Applica- tion Service	2.x, 1.x	Affected	Yes	VMSA-2021- 0028.1 (vmware.com)			12/12/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
VMware	Single Sign-On for VMware Tanzu Application Service	1.x	Affected	No	VMSA-2021- 0028.1 (vmware.com)			12/12/2021
VMware	Spring Cloud Gateway for Kubernetes	1.x	Affected	No	VMSA-2021- 0028.1 (vmware.com)			12/12/2021
VMware	Spring Cloud Gateway for VMware Tanzu	1.x	Affected	No	VMSA-2021- 0028.1 (vmware.com)			12/12/2021
VMware	Spring Cloud Services for VMware Tanzu	3.x	Affected	No	VMSA-2021- 0028.1 (vmware.com)			12/12/2021
VMware	VMware Carbon Black Cloud Workload Appliance	1.x	Affected	No	VMSA-2021- 0028.1 (vmware.com)			12/12/2021
VMware	VMware Carbon Black EDR Server	7.x, 6.x	Affected	No	VMSA-2021- 0028.1 (vmware.com)			12/12/2021
VMware	VMware Cloud Foundation	4.x, 3.x	Affected	No	VMSA-2021- 0028.1 (vmware.com)			12/12/2021
VMware		4.x, 3.x	Affected	No	VMSA-2021- 0028.1 (vmware.com)			12/12/2021
VMware	VMware Horizon	8.x, 7.x	Affected	Yes	VMSA-2021- 0028.4 (vmware.com)		VMware KB 87073 (vmware.com)	12/17/2021
VMware	VMware Horizon Cloud Connector	1.x, 2.x	Affected	Yes	VMSA-2021- 0028.1 (vmware.com)			12/12/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
VMware	VMware Horizon DaaS	9.1.x, 9.0.x	Affected	No	VMSA-2021- 0028.1 (vmware.com)			12/12/2021
VMware	VMware Identity Manager	3.3.x	Affected	No	VMSA-2021- 0028.1 (vmware.com)			12/12/2021
VMware	VMware NSX-T Data Centern	3.x, 2.x	Affected	No	VMSA-2021- 0028.1 (vmware.com)			12/12/2021
VMware	VMware Site Recovery Manager	8.x	Affected	No	VMSA-2021- 0028.1 (vmware.com)			12/12/2021
VMware	VMware Tanzu Application Service for VMs	2.x	Affected	No	VMSA-2021- 0028.1 (vmware.com)			12/12/2021
VMware	VMware Tanzu GemFire	9.x, 8.x	Affected	No	VMSA-2021- 0028.1 (vmware.com)			12/12/2021
VMware	VMware Tanzu Greenplum	6.x	Affected	No	VMSA-2021- 0028.1 (vmware.com)			12/12/2021
VMware	VMware Tanzu Kubernetes Grid Integrated Edition	1.x	Affected	No	VMSA-2021- 0028.1 (vmware.com)			12/12/2021
VMware	VMware Tanzu Observability by Wavefront Nozzle	3.x, 2.x	Affected	Yes	VMSA-2021- 0028.1 (vmware.com)			12/12/2021
VMware	VMware Tanzu Operations Manager	2.x	Affected	Yes	VMSA-2021- 0028.1 (vmware.com)			12/12/2021
VMware	VMware Tanzu SQL with MySQL for VMs	2.x, 1.x	Affected	No	VMSA-2021- 0028.1 (vmware.com)			12/12/2021

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes Other References	Last Updated
VMware	VMware Telco Cloud Automation	2.x, 1.x	Affected	No	VMSA-2021- 0028.1 (vmware.com)		12/12/2021
VMware	VMware Unified Access Gateway	21.x, 20.x, 3.x	Affected	No	(vmware.com) VMSA-2021- 0028.1 (vmware.com)		12/12/2021
VMware	VMware vCenter Cloud Gateway	1.x	Affected	No	VMSA-2021- 0028.1 (vmware.com)		12/12/2021
VMware	vCenter Server - OVA	7.x, 6.7.x, 6.5.x	Affected	Pending	VMSA-2021- 0028.4 (vmware.com)	Workaround © KB87081 (vmware.com)	2021-12-17
VMware	vCenter Server - Windows	6.7.x, 6.5.x	Affected	Pending	VMSA-2021- 0028.4 (vmware.com)	Workaround © KB87096 (vmware.com)	2021-12-17
VMware	VMware vRealize Automation	8.x, 7.x	Affected	No	VMSA-2021- 0028.1 (vmware.com)	(*)	12/12/2021
VMware	VMware vRealize Lifecycle Manager	8.x	Affected	No	VMSA-2021- 0028.1 (vmware.com)		12/12/2021
VMware	VMware vRealize Log Insight	8.x	Affected	No	VMSA-2021- 0028.1 (vmware.com)		12/12/2021
VMware	VMware vRealize Operations	8.x	Affected	No	VMSA-2021- 0028.1 (vmware.com)		12/12/2021
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

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
VMware	VMware Workspace ONE Access Connector (VMware Identity Manager Connector)	21.x, 20.10.x, 19.03.0.1	Affected	No	VMSA-2021- 0028.1 (vmware.com)			12/12/2021
Vyaire			Not Affected		Vyaire Advisory Link			12/22/2021
WAGO	WAGO Smart Script	4.2.x < 4.8.1.3	Affected	Yes	WAGO Website			12/17/2021
Wasp Barcode technologie WatchGuar Western Digital					Lab Mitigation Update Waspbarcode Assetcloud Inventorycloud 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 Pass- word Man- ager is affected		12/22/2021
WIBU Systems WindRiver	CodeMeter Cloud Lite	2.2 and prior	Affected	Yes	WIBU Systems Advisory Link Windriver			12/22/2021
WireShark Wistia WitFoo					Security Notice Gitlab Wireshark Wistia Incidents Witfoo Emergency			
WordPress					Update Wordpress			
Workspher	e				Support Workspace Security Update			
Wowza					Wowza Known Issues with Streaming Engine			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
XCP-ng					XCP lOG4j			
					Vulnerability			
XenForo					Xenforo PSA			
					Elasticsearch			
Xerox					Xerox Special			
					Bulletin			
VD (D					CVE-2021-44228			
XPertDoc					Xpertdoc			
XPLG					XPLG Secure			
XWIKI					Log4j Xwiki			
AWIKI					CVE-2021-44228			
Xylem	Aquatalk		Affected	Pacthing complete	Xylem Advisory			12/22/2021
Ayıcılı	Aquataik		Anctieu	1 actining complete	Link			14/44/4041
Xylem	Avensor		Affected	Pacthing complete	Xylem Advisory			12/22/2021
11 y 10111	11/011501		111100000	1 acoming complete	Link			12/22/2021
Xylem	Sensus		Affected	Pacthing complete	Xylem Advisory			12/22/2021
11,10111	Analytics		111100000	r detiming compress	Link			1-//
Xylem	Sensus Au-		Affected	Pacthing complete	Xylem Advisory			12/22/2021
V	tomation			3 1	Link			1 1
	Control							
	Configura-							
	tion change							
	complete							
Xylem	Sensus		Affected	Mitigation in process	Xylem Advisory			12/22/2021
	Cathodic				Link			
	Protection							
	Mitigation							
	in process							
	Mitigation .							
W 1	in process		A.C 1	D . 1:	V 1 41.			10/00/0001
Xylem	Sensus		Affected	Patching complete	Xylem Advisory			12/22/2021
	FieldLogic				Link			
Vylom	LogServer		A ffootod	Doothing complete	Vylom Advisor			19/99/9091
Xylem	Sensus Lighting		Affected	Pacthing complete	Xylem Advisory Link			12/22/2021
	Control				LIIIK			
Xylem	Sensus		Affected	Pacthing complete	Xylem Advisory			12/22/2021
2xy10111	NetMetrics		mouteu	1 acoming complete	Link			14/44/4041
	Configura-				Lim			
	tion change							
	complete							
Xylem	Sensus RNI	4.7 through 4.10,	Affected	Pacthing complete	Xylem Advisory			12/22/2021
J	Saas	4.4 through 4.6,		QF	Link			, -,
		4.2						

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Xylem	Sensus RNI On Prem	4.7 through 4.10, 4.4 through 4.6, 4.2	Affected	Mitigation in process	Xylem Advisory Link			12/22/2021
Xylem	Sensus SCS		Affected	Pacthing complete	Xylem Advisory Link			12/22/2021
Xylem	Smart Irrigation		Affected	Remediation in process	Xylem Advisory Link			12/22/2021
Xylem	Water Loss Manage- ment (Visenti)		Affected	Pacthing complete	Xylem Advisory Link			12/22/2021
Xylem	Configuration change complete	n	Affected	Pacthing complete	Xylem Advisory Link			12/22/2021
Xylem	Xylem Cloud		Affected	Pacthing complete	Xylem Advisory Link			12/22/2021
Xylem	Xylem Edge Gateway (xGW)		Affected	Pacthing complete	Xylem Advisory Link			12/22/2021
Yellowbrid YellowFin	k `				YellowBrick Security Advisory Yellowbrick YellowFinbi Notice Critical Vulnerability in			
YOKOGA	.WA		Under		Log4j YOKOGAWA			12/22/2021
YSoft			Investigati	on	Advisory Link Ysoft Safeq			
SAFEQ Zabbix ZAMMAI)				Zabbix Log4j Zammad Elasticsearch Users			
Zaproxy Zebra					Zaproxy Zebra lifeguard Security			

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Zendesk	All Products	All Versions	Affected	No	2021-12-13 Security Advisory - Apache Log4j (CVE-2021- 44228)	Zendesk products are all cloud-based; thus there are no updates for the customers to install as the company is working on patching their infrastructure and systems.		12/13/2021
Zenoss Zentera Systems, Inc. Zerto Zesty Zimbra Zoom ZPE systems	CoIP Access Platform	All	Not Affected		Zenoss [CVE-2021- 44228] Log4Shell Vulnerability in Apache Log4j Zerto KB Zesty Log4j Exploit BugZilla Zimbra Zoom Security Exposure ZpeSystems CVE-2021-44228			12/17/2021
Inc Zscaler	See Link (Multiple Products)		Not Affected	No	CVE-2021-44228 log4j Vulnerability			12/15/2012

Vendor	Product	Version(s)	Status	Update Available	Vendor Link	Notes	Other References	Last Updated
Zyxel					Zyxel Security Advisory for Apache Log4j			
Zyxel	Security Firewall/Ga	ZLD Firmware atewsystrity Services, Nebula	Not Affected	N/A	Zyxel Security Advisory			12/14/2021