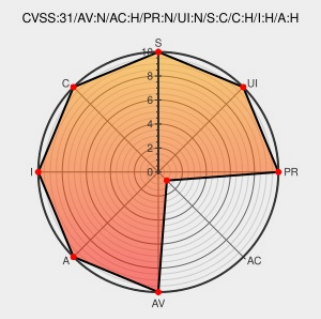
CVE-2021-45046

Published on: Not Yet Published

Last Modified on: 10/06/2022 02:54:00 AM UTC

CVE-2021-45046

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Log4j from Apache contain the following vulnerability:

It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. This could allows attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, $${ctx:loginId}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern resulting in an information leak and remote code execution in some environments and local code execution in all environments. Log4j 2.16.0 (Java 8) and 2.12.2 (Java 7) fix this issue by removing support for message lookup patterns and disabling JNDI functionality by default.

CVE-2021-45046 has been assigned by security@apache.org to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Apache Software Foundation** - **Apache Log4j** version **< 2.16.0**

CVSS3 Score: 9 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 5.1 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

PARTIAL | PARTIAL | PARTIAL

CVE References

Description	Tags	Link
	cert-portal.siemens.com application/pdf	CONFIRM cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf
Debian -- Security Information -- DSA-5022-1 apache-log4j2	www.debian.org Depreciated Link text/html	DEBIAN DSA-5022
Security Advisory	psirt.global.sonicwall.com text/html	CONFIRM psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0032
	cert-portal.siemens.com application/pdf	CONFIRM cert-portal.siemens.com/productcert/pdf/ssa-714170.pdf
oss-security - CVE-2021-45046: Apache Log4j2 Thread Context Message Pattern and Context Lookup Pattern vulnerable to a denial of service attack	www.openwall.com text/html	MLIST [oss-security] 20211214 CVE-2021-45046: Apache Log4j2 Thread Context Message Pattern and Context Lookup Pattern vulnerable to a denial of service attack
cve-website	www.cve.org text/html	MISC www.cve.org/CVERecord?id=CVE-2021-44228
Oracle Critical Patch Update Advisory - April 2022	www.oracle.com text/html	MISC www.oracle.com/security-alerts/cpuapr2022.html
oss-security - Re: CVE-2021-45046: Apache Log4j2 Thread Context Message Pattern and Context Lookup Pattern vulnerable to a denial of service attack	www.openwall.com text/html	MLIST [oss-security] 20211215 Re: CVE-2021-45046: Apache Log4j2 Thread Context Message Pattern and Context Lookup Pattern vulnerable to a denial of service attack
[SECURITY] Fedora 35 Update: log4j-2.17.0-1.fc35 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-abbe24e41c
Oracle Critical Patch Update Advisory - January 2022	www.oracle.com text/html	MISC www.oracle.com/security-alerts/cpujan2022.html
Vulnerabilities in Apache Log4j Library Affecting Cisco Products: December 2021	tools.cisco.com text/html	CISCO 20211210 Vulnerabilities in Apache Log4j Library Affecting Cisco Products: December 2021
oss-security - Re: CVE-2021-45046: Apache Log4j2 Thread Context Message Pattern and Context Lookup Pattern vulnerable to a denial of service attack	www.openwall.com text/html	MLIST [oss-security] 20211215 Re: CVE-2021-45046: Apache Log4j2 Thread Context Message Pattern and Context Lookup Pattern vulnerable to a denial of service attack
INTEL-SA-00646	www.intel.com text/html	CONFIRM www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00646.html
	cert-portal.siemens.com application/pdf	CONFIRM cert-portal.siemens.com/productcert/pdf/ssa-479842.pdf
	cert-portal.siemens.com application/pdf	CONFIRM cert-portal.siemens.com/productcert/pdf/ssa-397453.pdf
oss-security - Re: CVE-2021-45046: Apache Log4j2 Thread Context Message Pattern and Context Lookup Pattern vulnerable to a denial of service attack	www.openwall.com text/html	MLIST [oss-security] 20211218 Re: CVE-2021-45046: Apache Log4j2 Thread Context Message Pattern and Context Lookup Pattern vulnerable to a denial of service attack
Oracle Security Alert Advisory - CVE-2021-44228	www.oracle.com text/html	CONFIRM www.oracle.com/security-alerts/alert-cve-2021-44228.html

CVE-2021-45046 Apache Log4j Vulnerability in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20211215-0001/
Log4j – Apache Log4j Security Vulnerabilities	logging.apache.org text/html	MISC logging.apache.org/log4j/2.x/security.html
[SECURITY] Fedora 34 Update: log4j-2.17.0-1.fc34 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-5c9d12a93e
VU#930724 - Apache Log4j allows insecure JNDI lookups	www.kb.cert.org text/html	CERT-VN VU#930724
Oracle Critical Patch Update Advisory - July 2022	www.oracle.com text/html	MISC www.oracle.com/security-alerts/cpujul2022.html

Related QID Numbers

178942 Debian Security Update for apache-log4j2 (DSA 5022-1)

198606 Ubuntu Security Notification for Apache Log4j 2 Vulnerability (USN-5197-1)

20252 IBM DB2 Security Update for Log4j (6528672,6549888)

216275 VMware vCenter Server 7.0 Apache Log4j Remote Code Execution (RCE) Vulnerability (VMSA-2021-0028)

216276 VMware vCenter Server 6.7 Apache Log4j Remote Code Execution (RCE) Vulnerability (VMSA-2021-0028)

216277 VMware vCenter Server 6.5 Apache Log4j Remote Code Execution (RCE) Vulnerability (VMSA-2021-0028)

240209 Red Hat Update for JBoss Enterprise Application Platform 7.4.4 (RHSA-2022:1296)

240210 Red Hat Update for JBoss Enterprise Application Platform 7.4.4 (RHSA-2022:1297)

282198 Fedora Security Update for log4j (FEDORA-2021-5c9d12a93e) (Log4Shell)

282200 Fedora Security Update for log4j (FEDORA-2021-abbe24e41c) (Log4Shell)

317120 Cisco Unified Communications Manager (CUCM) Apache Log4j Vulnerability (cisco-sa-apache-log4j-qRuKNEbd)

317121 Cisco Unified Communications Manager IM and Presence Service (formerly CUPS) Apache Log4j Vulnerability (cisco-sa-apache-log4j-qRuKNEbd)

317123 Cisco UCS Central Software Apache Log4j Vulnerability (cisco-sa-apache-log4j-qRuKNEbd)

353084 Amazon Linux Security Advisory for aws-kinesis-agent : ALAS2-2021-1730

353085 Amazon Linux Security Advisory for java-1.8.0-openjdk, java-1.7.0-openjdk, java-1.6.0-openjdk : ALAS-2021-1553

353086 Amazon Linux Security Advisory for java-11-openjdk : ALAS2JAVA-OPENJDK11-2021-001

353087 Amazon Linux Security Advisory for java-1.8.0-amazon-corretto : ALAS2CORRETTO8-2021-001

353088 Amazon Linux Security Advisory for java-17-amazon-corretto, java-11-amazon-corretto, java-1.8.0-openjdk, java-1.7.0-openjdk : ALAS2-2021-1731

376178 Apache Log4j Remote Code Execution (RCE) Vulnerability (CVE-2021-45046)

376183 VMware NSX-T Apache Log4j Remote Code Execution (RCE) Vulnerability (VMSA-2021-0028)

376184 VMware Identity Manager (vIDM) and Workspace ONE Access Apache Log4j Remote Code Execution (RCE) Vulnerability (VMSA-2021-0028)

376185 DataDog Agent Log4j Remote Code Execution (RCE) Vulnerability

376192 Elasticsearch Logstash Log4j Remote Code Execution (RCE) Vulnerability

376193 Apache Log4j Remote Code Execution (RCE) Vulnerability (Log4Shell) Detected Based on Qualys Log4j scan Utility (CVE-2021-45046)

376207 VMware Horizon Windows Agent Apache Log4j Remote Code Execution (RCE) Vulnerabilities (VMSA-2021-0028) (Log4Shell)

376230 Dell EMC NetWorker Apache Log4j multiple Remote Code Execution (RCE) Vulnerabilities (DSA-2021-280)

376231 Dell EMC NetWorker Server Apache Log4j multiple Remote Code Execution (RCE) Vulnerabilities (DSA-2021-280)

376245 VMware Tanzu GemFire Log4j Remote Code Execution (RCE) Vulnerability (VMSA-2021-0028) (Log4Shell)

376261 VMware vRealize Orchestrator, VMware vRealize Automation and VMware vRealize Lifecycle Manager Log4j Remote Code Execution (RCE) Vulnerability (VMSA-2021-0028) (Log4Shell)

376267 Tableau Server and Desktop Multiple Vulnerabilities (Log4Shell)

376406 Adobe ColdFusion advisory for Apache Log4j Vulnerability (Log4Shell)

376415 IBM WebSphere Application Server Multiple Vulnerabilities (Log4Shell) (6526750)

376417 VMware Horizon Connection Server Apache Log4j Remote Code Execution (RCE) Vulnerabilities (VMSA-2021-0028) (Log4Shell)

376450 Symantec Endpoint Protection Manager (SEPM) Log4j Vulnerability (SYMSA19793)

376477 Autonomous Health Framework (AHF) Multiple Vulnerabilities (Log4Shell) (Doc ID 2828415.1)

590619 Siemens SENTRON Powermanager Apache Log4j Denial of Service (DoS) Vulnerability (SSA-661247) (Log4Shell)

590638 Schneider Electric EcoStruxure IT Gateway Apache Log4j Vulnerability (Log4Shell) (SESB-2021-347-01)

690752 Free Berkeley Software Distribution (FreeBSD) Security Update for graylog (650734b2-7665-4170-9a0a-eeced5e10a5e)

690757 Free Berkeley Software Distribution (FreeBSD) Security Update for opensearch (b0f49cb9-6736-11ec-9eea-589cfc007716) (Log4Shell)

730303 Apache Flink Emergency Release for Apache Log4j Vulnerability (Log4Shell)

730317 VMware Horizon Windows and Linux Agent Apache Log4j Remote Code Execution (RCE) Vulnerabilities (Unauthenticated Check) (Log4Shell)

730318 Palo Alto Networks (PAN-OS) Log4j Multiple Vulnerabilities (PAN-184592) (Log4Shell)

730329 Dell EMC NetWorker Virtual Edition Multiple Apache Log4j Remote Code Execution (RCE) Vulnerabilities (DSA-2021-280)

730331 Dell EMC NetWorker Virtual Edition multiple Apache Log4j Remote Code Execution (RCE) Vulnerabilities (DSA-2021-280)

730362 Neo4j Database Server Affected by Apache Log4j Security Vulnerability

730367 Dell EMC SRM Remote Code Execution (RCE) Vulnerability (DSA-2021-301)

730371 McAfee Web Gateway Multiple Vulnerabilities (WP-3335,WP-4131,WP-4159,WP-4237,WP-4259,WP-4329,WP-4348,WP-4355,WP-4376,WP-4407,WP-4421)

751493 OpenSUSE Security Update for log4j (openSUSE-SU-2021:4107-1)

751536 OpenSUSE Security Update for log4j (openSUSE-SU-2021:1601-1) (Log4Shell)

87473 Cisco Nexus Dashboard Fabric Controller (Formerly DCNM) Apache Log4j Vulnerability (cisco-sa-apache-log4j-qRuKNEbd)

Exploit/POC from Github

Rapidly scan filesystems for Java programs potentially vulnerable to Log4Shell (CVE-2021-44228) or "that Log4j JNDI e…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Log4j	All	All	All	All
Application	Apache	Log4j	2.0	-	All	All
Application	Apache	Log4j	2.0	beta9	All	All
Application	Apache	Log4j	2.0	rc1	All	All
Application	Apache	Log4j	2.0	rc2	All	All
Application	Apache	Log4j	All	All	All	All
Application	Arubanetworks	Silver Peak Orchestrator	-	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Intel	Audio Development Kit	-	All	All	All
Application	Intel	Computer Vision Annotation Tool	-	All	All	All
Application	Intel	Datacenter Manager	-	All	All	All
Application	Intel	Genomics Kernel Library	-	All	All	All
Application	Intel	Oneapi	-	All	All	All
Application	Intel	Secure Device Onboard	-	All	All	All
Application	Intel	Sensor Solution Firmware Development Kit	-	All	All	All
Application	Intel	System Debugger	-	All	All	All
Application	Intel	System Studio	-	All	All	All
Application	Netapp	Brocade San Navigator	-	All	All	All
Application	Netapp	Cloud Insights Acquisition Unit	-	All	All	All
Application	Netapp	Cloud Manager	-	All	All	All
Application	Netapp	Cloud Secure Agent	-	All	All	All
Application	Netapp	Oncommand Insight	-	All	All	All

Application	Netapp	Ontap Tools	-	All	All	All
Application	Netapp	Snapcenter	-	All	All	All
Hardware	Siemens	6bk1602-0aa12-0tp0	-	All	All	All
Operating System	Siemens	6bk1602-0aa12-0tp0 Firmware	All	All	All	All
Hardware	Siemens	6bk1602-0aa22-0tp0	-	All	All	All
Operating System	Siemens	6bk1602-0aa22-0tp0 Firmware	All	All	All	All
Hardware	Siemens	6bk1602-0aa32-0tp0	-	All	All	All
Operating System	Siemens	6bk1602-0aa32-0tp0 Firmware	All	All	All	All
Hardware	Siemens	6bk1602-0aa42-0tp0	-	All	All	All
Operating System	Siemens	6bk1602-0aa42-0tp0 Firmware	All	All	All	All
Hardware	Siemens	6bk1602-0aa52-0tp0	-	All	All	All
Operating System	Siemens	6bk1602-0aa52-0tp0 Firmware	All	All	All	All
Application	Siemens	Capital	-	All	All	All
Application	Siemens	Captial	All	All	All	All
Application	Siemens	Captial	2019.1	-	All	All
Application	Siemens	Captial	2019.1	sp1912	All	All
Application	Siemens	Comos	All	All	All	All
Application	Siemens	Cosmos	-	All	All	All
Application	Siemens	Desigo Cc Advanced Reports	4.0	All	All	All
Application	Siemens	Desigo Cc Advanced Reports	4.1	All	All	All
Application	Siemens	Desigo Cc Advanced Reports	4.2	All	All	All
Application	Siemens	Desigo Cc Advanced Reports	5.0	All	All	All
Application	Siemens	Desigo Cc Advanced Reports	5.1	All	All	All
Application	Siemens	Desigo Cc Info Center	5.0	All	All	All
Application	Siemens	Desigo Cc Info Center	5.1	All	All	All
Application	Siemens	Desigo Consumption Control Advanced Reporting	All	All	All	All
Application	Siemens	Desigo Consumption Control Advanced Reporting	-	All	All	All
Application	Siemens	Desigo Consumption Control Advanced Reporting	4.0	All	All	All
Application	Siemens	Desigo Consumption Control Advanced Reporting	4.1	All	All	All
Application	Siemens	Desigo Consumption Control Advanced Reporting	4.2	All	All	All
Application	Siemens	Desigo Consumption Control Advanced Reporting	5.0	All	All	All
Application	Siemens	Desigo Consumption Control Advanced Reporting	5.1	All	All	All

Application	Siemens	Desigo Consumption Control Info Center	5.0	All	All	All
Application	Siemens	Desigo Consumption Control Info Center	5.1	All	All	All
Operating System	Siemens	Dynamic Security Assessment	4.2	All	All	All
Operating System	Siemens	Dynamic Security Assessment	4.3	All	All	All
Operating System	Siemens	Dynamic Security Assessment	4.4	All	All	All
Application	Siemens	E-car Operating Center	All	All	All	All
Application	Siemens	E-car Operation Center	All	All	All	All
Application	Siemens	Energyip	8.5	All	All	All
Application	Siemens	Energyip	8.6	All	All	All
Application	Siemens	Energyip	8.7	All	All	All
Application	Siemens	Energyip	9.0	All	All	All
Application	Siemens	Energyip Prepay	3.7	All	All	All
Application	Siemens	Energyip Prepay	3.8	All	All	All
Application	Siemens	Energy Engage	3.1	All	All	All
Application	Siemens	Gma-manager	All	All	All	All
Application	Siemens	Head-end System Universal Device Integration System	All	All	All	All
Application	Siemens	Head-end System Universal Device Integration System	-	All	All	All
Application	Siemens	Industrial Edge Management	All	All	All	All
Application	Siemens	Industrial Edge Management	-	All	All	All
Operating System	Siemens	Industrial Edge Management	-	All	All	All
Application	Siemens	Industrial Edge Management Hub	All	All	All	All
Operating System	Siemens	Industrial Edge Manangement Hub	-	All	All	All
Application	Siemens	Logo! Soft Comfort	All	All	All	All
Operating System	Siemens	Logo! Soft Comfort	-	All	All	All
Application	Siemens	Mendix	All	All	All	All
Operating System	Siemens	Mendix	-	All	All	All
Application	Siemens	Mindsphere	All	All	All	All
Operating System	Siemens	Mindsphere	All	All	All	All
Application	Siemens	Navigator	All	All	All	All
Application	Siemens	Nx	All	All	All	All
Operating	Siemens	Nx	-	All	All	All

System						
Operating System	Siemens	Opcenter Intelligence	All	All	All	All
Application	Siemens	Opcenter Intelligence	All	All	All	All
Operating System	Siemens	Operation Scheduler	All	All	All	All
Application	Siemens	Operation Scheduler	All	All	All	All
Application	Siemens	Sentron Powermanager	4.1	All	All	All
Application	Siemens	Sentron Powermanager	4.2	All	All	All
Application	Siemens	Siguard Dsa	4.2	All	All	All
Application	Siemens	Siguard Dsa	4.3	All	All	All
Application	Siemens	Siguard Dsa	4.4	All	All	All
Application	Siemens	Simatic Wincc	7.4	All	All	All
Application	Siemens	Sipass Integrated	2.80	All	All	All
Application	Siemens	Sipass Integrated	2.85	All	All	All
Application	Siemens	Siveillance Command	All	All	All	All
Application	Siemens	Siveillance Control	All	All	All	All
Application	Siemens	Siveillance Control Pro	All	All	All	All
Application	Siemens	Siveillance Identity	1.5	All	All	All
Application	Siemens	Siveillance Identity	1.6	All	All	All
Application	Siemens	Siveillance Vantage	All	All	All	All
Application	Siemens	Siveillance Vantage	-	All	All	All
Application	Siemens	Siveillance Viewpoint	All	All	All	All
Application	Siemens	Solid Edge Cam Pro	All	All	All	All
Application	Siemens	Solid Edge Harness Design	All	All	All	All
Application	Siemens	Solid Edge Harness Design	2020	All	All	All
Application	Siemens	Solid Edge Harness Design	2020	-	All	All
Application	Siemens	Solid Edge Harness Design	2020	sp2002	All	All
Application	Siemens	Solid Edge Wiring Harness Design	-	All	All	All
Application	Siemens	Spectrum Power 4	All	All	All	All
Application	Siemens	Spectrum Power 4	4.70	-	All	All
Application	Siemens	Spectrum Power 4	4.70	sp7	All	All
Application	Siemens	Spectrum Power 4	4.70	sp8	All	All
Application	Siemens	Spectrum Power 7	All	All	All	All
Application	Siemens	Spectrum Power 7	-	All	All	All
Application	Siemens	Spectrum Power 7	2.30	All	All	All

Application	Siemens	Spectrum Power 7	2.30	-	All	All
Application	Siemens	Spectrum Power 7	2.30	sp2	All	All
Hardware	Siemens	Sppa-t3000 Ses3000	-	All	All	All
Operating System	Siemens	Sppa-t3000 Ses3000 Firmware	All	All	All	All
Application	Siemens	Teamcenter	All	All	All	All
Application	Siemens	Teamcenter Suite	-	All	All	All
Application	Siemens	Tracealertserverplus	All	All	All	All
Application	Siemens	Vesys	All	All	All	All
Application	Siemens	Vesys	-	All	All	All
Application	Siemens	Vesys	2019.1	All	All	All
Application	Siemens	Vesys	2019.1	-	All	All
Application	Siemens	Vesys	2019.1	sp1912	All	All
Application	Siemens	Xpedition Enterprise	-	All	All	All
Application	Siemens	Xpedition Enterprise Data Management	All	All	All	All
Application	Siemens	Xpedition Package Integrator	-	All	All	All
Application	Siemens	Xpedition Package Integrator	All	All	All	All
Application	Sonicwall	Email Security	All	All	All	All

cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:-:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:beta9:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:2.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*:

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

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

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

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

cpe:2.3:o:fedoraproject:fedora:34:*:*:*:*:*:*:*:

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

cpe:2.3:a:intel:audio_development_kit:-:*:*:*:*:*:*:*:

cpe:2.3:a:intel:computer_vision_annotation_tool:-:*:*:*:*:*:*:*:

cpe:2.3:a:intel:datacenter_manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:intel:datacenter_manager:-:*:*:*:*:*:*:*:

cpe:2.3:a:intel:genomics_kernel_library:-:*:*:*:*:*:*:*:

cpe:2.3:a:intel:oneapi:-:*:*:*:*:eclipse:*:*:

cpe:2.3:a:intel:secure_device_onboard:-:*:*:*:*:*:*:*:

cpe:2.3:a:intel:sensor_solution_firmware_development_kit:-:*:*:*:*:*:*:*:

cpe:2.3:a:intel:system_debugger:-:*:*:*:*:*:*:*:

cpe:2.3:a:intel:system_studio:-:*:*:*:*:*:*:*:

cpe:2.3:a:netapp:brocade_san_navigator:-:*:*:*:*:*:*:*:

cpe:2.3:a:netapp:cloud_insights_acquisition_unit:-:*:*:*:*:*:*:*:

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

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

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

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

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

cpe:2.3:h:siemens:6bk1602-0aa12-0tp0:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:6bk1602-0aa12-0tp0_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:6bk1602-0aa22-0tp0:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:6bk1602-0aa22-0tp0_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:6bk1602-0aa32-0tp0:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:6bk1602-0aa32-0tp0_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:6bk1602-0aa42-0tp0:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:6bk1602-0aa42-0tp0_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:6bk1602-0aa52-0tp0:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:6bk1602-0aa52-0tp0_firmware:*:*:*:*:*:*:*:*:

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

cpe:2.3:a:siemens:captial:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:captial:2019.1:-:*:*:*:*:*:*:

cpe:2.3:a:siemens:captial:2019.1:sp1912:*:*:*:*:*:*:

cpe:2.3:a:siemens:comos:*:*:*:*:*:*:*:*:

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

cpe:2.3:a:siemens:desigo_cc_advanced_reports:4.0:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_cc_advanced_reports:4.1:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_cc_advanced_reports:4.2:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_cc_advanced_reports:5.0:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_cc_advanced_reports:5.1:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_cc_info_center:5.0:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_cc_info_center:5.1:*:*:*:*:*:*:*:

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

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

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

cpe:2.3:a:siemens:desigo_consumption_control_advanced_reporting:4.1:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_consumption_control_advanced_reporting:4.2:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_consumption_control_advanced_reporting:5.0:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_consumption_control_advanced_reporting:5.1:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_consumption_control_info_center:5.0:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:desigo_consumption_control_info_center:5.1:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:dynamic_security_assessment:4.2:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:dynamic_security_assessment:4.3:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:dynamic_security_assessment:4.4:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:e-car_operating_center:*:*:*:*:cloud:*:*:*:

cpe:2.3:a:siemens:e-car_operation_center:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:energyip:8.5:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:energyip:8.6:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:energyip:8.7:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:energyip:9.0:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:energyip_prepay:3.7:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:energyip_prepay:3.8:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:energy_engage:3.1:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:gma-manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:head-end_system_universal_device_integration_system:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:head-end_system_universal_device_integration_system:-:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:industrial_edge_management:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:industrial_edge_management:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:industrial_edge_management:-:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:industrial_edge_management_hub:*:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:industrial_edge_manangement_hub:-:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:logo\!_soft_comfort:*:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:logo\!_soft_comfort:-:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:mendix:*:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:mendix:-:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:mindsphere:*:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:mindsphere:*:*:*:*:cloud:*:*:*:

cpe:2.3:a:siemens:navigator:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:nx:*:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:nx:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:opcenter_intelligence:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:opcenter_intelligence:*:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:operation_scheduler:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:operation_scheduler:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:sentron_powermanager:4.1:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:sentron_powermanager:4.2:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:siguard_dsa:4.2:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:siguard_dsa:4.3:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:siguard_dsa:4.4:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simatic_wincc:7.4:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:sipass_integrated:2.80:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:sipass_integrated:2.85:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:siveillance_command:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:siveillance_control:*:*:*:*:pro:*:*:*:

cpe:2.3:a:siemens:siveillance_control_pro:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:siveillance_identity:1.5:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:siveillance_identity:1.6:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:siveillance_vantage:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:siveillance_vantage:-:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:siveillance_viewpoint:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:solid_edge_cam_pro:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:solid_edge_harness_design:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:solid_edge_harness_design:2020:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:solid_edge_harness_design:2020:-:*:*:*:*:*:*:

cpe:2.3:a:siemens:solid_edge_harness_design:2020:sp2002:*:*:*:*:*:*:

cpe:2.3:a:siemens:solid_edge_wiring_harness_design:-:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:spectrum_power_4:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:spectrum_power_4:4.70:-:*:*:*:*:*:*:

cpe:2.3:a:siemens:spectrum_power_4:4.70:sp7:*:*:*:*:*:*:

cpe:2.3:a:siemens:spectrum_power_4:4.70:sp8:*:*:*:*:*:*:

cpe:2.3:a:siemens:spectrum_power_7:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:spectrum_power_7:-:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:spectrum_power_7:2.30:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:spectrum_power_7:2.30:-:*:*:*:*:*:*:

cpe:2.3:a:siemens:spectrum_power_7:2.30:sp2:*:*:*:*:*:*:

cpe:2.3:h:siemens:sppa-t3000_ses3000:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:sppa-t3000_ses3000_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:teamcenter:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:teamcenter_suite:-:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:tracealertserverplus:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:vesys:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:vesys:-:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:vesys:2019.1:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:vesys:2019.1:-:*:*:*:*:*:*:

cpe:2.3:a:siemens:vesys:2019.1:sp1912:*:*:*:*:*:*:

cpe:2.3:a:siemens:xpedition_enterprise:-:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:xpedition_enterprise_data_management:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:xpedition_package_integrator:-:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:xpedition_package_integrator:*:*:*:*:*:*:*:*:

cpe:2.3:a:sonicwall:email_security:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@freeformz	cve.org/CVERecord?id=C… TL;DR: 2.16.0 or bust	2021-12-14 18:04:01
@theprincessxena	New CVE issued: CVE-2021-45046	2021-12-14 18:26:42
@_r_netsec	Previous log4j patch insufficient in some situations. New CVE posted and new log4j released 2.16.	2021-12-14 18:28:06
@nellaiomar	@sjmaple @sjmaple How much impact is this?	2021-12-14 19:37:49
@techsolvency	log4j 2.1.15 CVE-2021-45046: "The fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain… twitter.com/i/web/status/1…	2021-12-14 19:40:09
@dragosr	CVE-2021-45046 = Log4JarJarBinks?	2021-12-14 19:40:59
@nocksers	@justizin Published like an hour or so ago	2021-12-14 19:41:10
@Libranalysis	AndroidProjectCreator 1.5.2-stable updates its #log4j dependency to version 2.16.0 to remediate CVE-2021-45046, whi… twitter.com/i/web/status/1…	2021-12-14 19:41:40
@KevinSMcArthur	asdf... CVE-2021-45046 just... faaasdasdasdfasd	2021-12-14 19:42:27
@sjvn	@lorenc_dan Yep:	2021-12-14 19:43:12
@x0rz	PSA - CVE-2021-45046: setting `log4j2.noFormatMsgLookup` to `true` do NOT mitigate this specific vulnerability	2021-12-14 19:47:57
@BenBremert	@Akoneira cve.org/CVERecord?id=C… ?	2021-12-14

@BenBrenner	@Akroneira cve.org/CVERecord?id=C…	2021-12-14 19:51:17
@SecurePeacock	CVE-2021-45046: It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certai… twitter.com/i/web/status/1…	2021-12-14 19:57:24
@marcwrogers	Previous fix for log4j 2.15.0 was incomplete in certain non default configurations so a new CVE raised: CVE-2021-45046.	2021-12-14 20:01:30
@LunaSecIO	We just updated our Mitigation Guide with the 2nd log4j vulnerability (CVE-2021-45046). It's RCE for log4j <=2.14.… twitter.com/i/web/status/1…	2021-12-14 21:08:54
@yigalatz	We validated that this hotpatch also addresses CVE-2021-45046 lists.apache.org/thread/83y7dx5… Stay tuned for readme update… twitter.com/i/web/status/1…	2021-12-14 21:14:07
@orehcelE	Equisde	2021-12-14 21:14:45
@jd_is_lost	Well... Shit.	2021-12-14 21:18:22
@rlove	Hey everyone we heard you liked last Friday so much we're gonna have you do it again #log4j cve.org/CVERecord?id=C…	2021-12-14 21:22:12
@KWF	CVE-2021-45046 in log4j v2.15.0. So in case you were still on the fence; computers were a mistake.	2021-12-14 21:23:39
@itseccolin	New Log4j CVE published today: CVE-2021-45046 https://t.co/j19NbMB99k	2021-12-14 21:25:13
@oliverandrich	Nun...	2021-12-14 21:27:21
@JensJacobsson	Ding ding ding ...prepare for round 2 ?	2021-12-14 21:31:47
@jboulineau	The fix for log4j is broken.	2021-12-14 21:34:33
@yama_bong	apacheのサイト上でCVSS スコア 3.7の新しい脆弱性 CVE-2021-45046 が公開されたらしい。 logging.apache.org/log4j/2.x/secu… twitter.com/ymmt2005/statu…	2021-12-14 22:39:57
@darkmastermindz	Literally 2 hours ago	2021-12-14 22:43:38
@Darkarnium	Just added rules for #log4j CVE-2021-45046! This rule looks for an Interpolator class which does not contain a Jnd… twitter.com/i/web/status/1…	2021-12-14 22:49:44
@Darkarnium	Please keep in mind that CVE-2021-45046 appears to only provide a DoS vector, rather than code execution (currently… twitter.com/i/web/status/1…	2021-12-14 22:50:02
@dchatenay	Move over CVE-2021-44228, hello CVE-2021-45046	2021-12-14 22:52:32
@jrconlin	Heads up. if you patched up log4j, you probably need to patch up log4j. New CVE: Software… twitter.com/i/web/status/1…	2021-12-14 22:56:20
@ukeer	Oh. ein CVE fuer log4j 2.15. *sigh* kann nicht sagen dass ich ueberrascht bin	2021-12-14 22:58:04
@kadumuller	E você achando que atualizou o log4j e estava descansando pro final de ano achou errado	2021-12-14 22:58:10
@AlexaChenowith	Previous log4j patch insufficient in some situations. New CVE posted and new log4j released 2.16.	2021-12-14 23:00:03
@WilfridBlanc	Previous log4j patch insufficient in some situations. New #CVE posted and new log4j released 2.16.	2021-12-14 23:00:03

@repeatedly	log4j2のアップデート，2.15.0にするだけだと完全じゃないらしい．新しいCVEが出来てて，2.16.0にするのが推奨されている >	2021-12-14 23:02:29
@_deftoner_	#log4j #CVE-2021-44228 #CVE-2021-45046 https://t.co/r0zLl9OIWD	2021-12-14 23:03:54
@mockalist	@JoernBoegeholz Not good enough to be on 2.15.0.	2021-12-14 23:12:39
@reddit_progr	Log4Shell round 2 /post reddit.com/r/programming/…	2021-12-14 23:14:03
@fujiwara	log4j2.noFormatMsgLookup=trueでは防げないDoS / “CVE - CVE-2021-45046” htn.to/25CcinSYRv	2021-12-15 00:11:44
@nagise	CVE-2021-45046 よく分かんないな。 SystemProperty のスイッチだけの対応では不完全という趣旨のようだが……? まあ基本的にはライブラリをバージョンアップしろ、なんだと思うが。	2021-12-15 00:11:44
@making	Logbackの脆弱性と言われているものは無視していいレベルの実現性だけど、 Log4j2の新しいCVEは2.16.0にバージョンアップしないとダメそう。 環境変数設定で対応終わったと思ったみなさん、もう一踏ん張りです	2021-12-15 00:18:25
@PerfectBoatJP	CVE-2021-45046	2021-12-15 00:19:22
@yuki_kawamitsu	次から次にクリスマス休暇時に大変だなこりゃ... CVE-2021-45046	2021-12-15 00:22:05
@defenceability	これか...2.15.0じゃなくて2.16.0に上げろってことね。 log4j 1系の後継かそうじゃないか問題はもう少し静観。	2021-12-15 00:23:25
@sutest1101	CVE - CVE-2021-45046	2021-12-15 00:26:30
@yamadamn	CVE-2021-45046 によると、CVE-2021-44228に対処するための Log4j 2.15.0 の修正はデフォルト以外の特定の構成では不完全で -Dlog4j2.fo… twitter.com/i/web/status/1…	2021-12-15 00:31:08
@minamijoyo	2件のコメント “CVE - CVE-2021-45046” htn.to/3VQGNaSHUm	2021-12-15 00:32:25
@cheva	あらら / “CVE - CVE-2021-45046” htn.to/4rsvLrSouT	2021-12-15 00:34:05
@kzm	log4j 2.16.0 が出たのは CVE-2021-45046 のせいかな。	2021-12-15 00:35:08
@thejonmccoy	A second CVE entry to follow up and n Log4J And this maps 3rd party applications that are… twitter.com/i/web/status/1…	2021-12-15 00:35:08
@stockholmux	A new version of OpenSearch will be released that updates Log4j 2.15.0 -> Log4j 2.16.0 due to CVE-2021-45046 (yup,… twitter.com/i/web/status/1…	2021-12-15 00:36:32
@yamadamn	CVE-2021-45046はRCEではなくDOSを引き起こす可能性がある模様。 引用RT元によれば、Amazon Correttoチームの作成したLog4jHotPatchなどを利用することでも、一旦は回避できそうでもある。 github.com/corretto/hotpa…	2021-12-15 00:41:45
@minamijoyo	CVE-2021-44228(Log4Shell)対策でlog4j2.noFormatMsgLookup=trueで回避という情報があったけど、特定の条件下では防ぎきれないパターンがあるようでCVE-2021-45046として別に… twitter.com/i/web/status/1…	2021-12-15 00:43:47
@ThierryDelaitre	Hope it covers the new log4j recent addition of CVE-2021-45046 as well #Log4Shell twitter.com/qualys/status/…	2021-12-15 00:47:47
@suzu_GBA2003	log4j 2.15.0じゃあ足りんかったんか cve.org/CVERecord?id=C…	2021-12-15 00:48:06
@dblockdotorg	We got so fast at releasing OpenSearch, why not do another one for CVE-2021-45046?	2021-12-15

	#opensearch… twitter.com/i/web/status/1…	00:49:02
@magiauk	CVE - CVE-2021-45046 ift.tt/3F0iQ2k	2021-12-15 00:51:59
@buri_83	安全なバージョンとアナウンスされていた log4j 2.15 も完全じゃない。最新の2.16 にする必要がありそう。 cve.org/CVERecord?id=C…	2021-12-15 00:52:19
@luigy0x18	Así que la versión 2.15 no es un parche totalmente funcional ya sabéis a actualizar a la 2.16 ?	2021-12-15 00:53:09
@shen_car	2.15はCVE-2021-45046があるから、 2.16に更新するんやで。2.15にして安心じゃないので注意。	2021-12-15 01:31:27
@dblockdotorg	@_tallison Thanks for calling us out. Once we read CVE-2021-45046 it was clear that the safest and easiest to deal… twitter.com/i/web/status/1…	2021-12-15 01:35:17
@algnc	oh good. cve.org/CVERecord?id=C…	2021-12-15 01:36:00
@Santea3173	CVE-2021-45046 の方は OpenShift 4 は Not affected と。Red Hat さん情報早いな〜♪ access.redhat.com/security/cve/c…	2021-12-15 01:41:01
@8con	log4j 2.15 is also vulnerable(CVE-2021-45046) :(but, you can check this issue by using logpresso scanner twitter.com/8con/status/14…	2021-12-15 01:41:56
@MasafumiNegishi	Guide: How To Detect and Mitigate the Log4Shell Vulnerability (CVE-2021-44228 & CVE-2021-45046) | LunaSec lunasec.io/docs/blog/log4…	2021-12-15 01:43:25
@beewee22	cve.org/CVERecord?id=C… log4j 2.15 ..? ㅠㅠ	2021-12-15 01:43:37
@8con	log4j 2.15 . CVE-2021-45046 2.15 , . twitter.com/8con/status/14…	2021-12-15 01:43:40
@akino_R294	CVE-2021-45046出てるじゃん…	2021-12-15 01:46:52
@ywatai	2.15.0 の修正や設定での lookup の無効化だけだと context lookup や MDC を使っている場合は DoS れるよ、と。ふーむ？	2021-12-15 01:55:17
@kurtseifried	Good news: CVE-2021-45046 doesn't matter (DoS, nonstandard config), the hot patches work (github.com/cloudsecurityа…)… twitter.com/i/web/status/1…	2021-12-15 01:55:32
@anedwar	Thought you were done with log4j updates? https://t.co/lFENd3zPbe	2021-12-15 01:55:59
@chohkan	Guide: How To Detect and Mitigate the Log4Shell Vulnerability (CVE-2021-44228 & CVE-2021-45046) | LunaSec lunasec.io/docs/blog/log4…	2021-12-15 01:57:38
@gnomon	@Jedediah6 @TheASF I do:	2021-12-15 02:03:05
@muziyoshiz	aws.amazon.com/jp/security/se… CVE-2021-45046の記載はまだ無いなあ。もう1回アップデートがあるかもしれない	2021-12-15 02:03:37
@LunaSecIO	Here's our analysis and finding of the 2nd log4j vulnerability (CVE-2021-45046). We found this CVE still leaves you… twitter.com/i/web/status/1…	2021-12-15 02:05:13
@nharuki	Log4jの新しい脆弱性情報 (CVE-2021-45046) か！？ cve.org/CVERecord?id=C…	2021-12-15 02:05:45
@bongole	log4jのやつDOSできるやつも見つかったのか	2021-12-15 02:10:13
@w0mbat5eoul	Deleted previous post. It was pointed out it could cause undo panic… New CVE: CVE-2021-45046… twitter.com/i/web/status/1…	2021-12-15 02:10:33
@kumakaba	あ、log4j 2.15.xでもダメなのかw cve.org/CVERecord?id=C…	2021-12-15

		02:14:12
@ohhara_shiojiri	NVD - CVE-2021-45046	2021-12-15 02:14:41
@accessfinder	@_mattata How is CVE-2021-45046 #Log4Shell2 if it requires non-default configuration and "only" leads to DOS not RCE?	2021-12-15 02:14:49
@ohhara_shiojiri	CVE - CVE-2021-45046	2021-12-15 02:14:59
@hn_frontpage	Analysis of the 2nd Log4j CVE published earlier (CVE-2021-45046 / Log4Shell2) L: lunasec.io/docs/blog/log4… C: news.ycombinator.com/item?id=295615…	2021-12-15 03:01:45
@hncynic	Title: Analysis of the 2nd Log4j CVE published earlier (CVE-2021-45046 / Log4Shell2) ?: Can someone explain what this is supposed to do?	2021-12-15 03:01:54
@tammeke140674	Analysis of the 2nd Log4j CVE published earlier (CVE-2021-45046 / Log4Shell2) ift.tt/3pW2kds 3	2021-12-15 03:03:33
@knelsonvsi	Analysis of the 2nd Log4j CVE published earlier (CVE-2021-45046 / Log4Shell2) ift.tt/3pW2kds 3	2021-12-15 03:03:43
@radoncnotes	Analysis of the 2nd Log4j CVE published earlier (CVE-2021-45046 / Log4Shell2) ift.tt/3pW2kds 3	2021-12-15 03:05:48
@cdespinosa	@identd cve.org/CVERecord?id=C…	2021-12-15 03:07:24
@winsontang	Analysis of the 2nd Log4j CVE published earlier (CVE-2021-45046 / Log4Shell2) lunasec.io/docs/blog/log4… https://t.co/nf58zIiSno	2021-12-15 03:08:06
@akbarth3great	Analysis of the 2nd Log4j CVE published earlier (CVE-2021-45046 / Log4Shell2) dlvr.it/SFNvsb	2021-12-15 03:08:09
@sgtmuffin	Looks like there is a workaround for the Log4J CVE. cve.org/CVERecord?id=C…	2021-12-15 03:08:40
@HNTweets	Analysis of the 2nd Log4j CVE published earlier (CVE-2021-45046 / Log4Shell2): lunasec.io/docs/blog/log4… Comments: news.ycombinator.com/item?id=295615…	2021-12-15 03:10:02
@Samadams812	At least it's not another RCE?	2021-12-15 03:15:01
@damon_berry	The gift that keeps on giving: twitter.com/decarboxy/stat…	2021-12-15 03:41:48
@sockety_v	もう使うのやめればいいのに＞ 「CVE-2021-45046」は、13日付けでリースされた「Log4j 2.16.0」で対処されている。システムプロパティ「log4j2.noFormatMsgLookup」を「true」に変更… twitter.com/i/web/status/1…	2021-12-15 03:46:56
@top_hn_bot	New top story! Poster: freeqaz Title: Analysis of the 2nd Log4j CVE published earlier (CVE-2021-45046 / Log4Shell2)… twitter.com/i/web/status/1…	2021-12-15 03:48:14
@Myinfosecfeed	New post: "Security Analysis of the 2nd Log4j CVE published earlier (CVE-2021-45046 / Log4Shell2)" ift.tt/3dQPs2q	2021-12-15 03:48:47
@dsewnr	lunasec.io/docs/blog/log4… ?	2021-12-15 03:51:46
@not_rogue	hm lunasec.io/docs/blog/log4…	2021-12-15 03:52:52
@DanCast	Why have one log4j bug, when you can have two at twice the price? lunasec.io/docs/blog/log4…	2021-12-15 04:52:33
@8con	supporting log4j 2.15.0 vulnerability(CVE-2021-45046) detection and zip file scanning	2021-12-15 04:55:02

@d_shimizu	? //	2021-12-15 05:05:07
@ollieatnccgroup	Pushed the days first #log4 #log4shell meta thread update: - Details of CVE-2021-45046 for 2.15.0 - need to upgrad… twitter.com/i/web/status/1…	2021-12-15 05:05:36
@zhuowei	No, you don't need to panic about CVE-2021-45046: 1) almost no app has a log4j2.xml with a ${ctx:variable} pattern… twitter.com/i/web/status/1…	2021-12-15 05:06:00
@noelgeorgi	@likethecoins new one	2021-12-15 05:12:55
@newsyc100	Analysis of the 2nd Log4j CVE published earlier (CVE-2021-45046 / Log4Sh bit.ly/3q0PPgA (bit.ly/3DWdovW)	2021-12-15 05:14:40
@japanese_afro	log4jがまだなおってなかったらしいw また報告上がってる lunasec.io/docs/blog/log4…	2021-12-15 05:17:54
@tenrobots	@phishy @WoogyChuck @CubicleApril Because Log4J CVE-2021-44228 and CVE-2021-45046 ?	2021-12-15 05:25:47
@CisoInvisible	Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released - invisibleciso.com/12349213/secon… https://t.co/WR3v5Hi8Fr	2021-12-15 06:19:23
@dareka252	2.15.0でも特定条件でDoS攻撃受けるぞって指摘されててワロタ twitter.com/dareka252/stat…	2021-12-15 06:20:01
@ToivoVoll	…and here we go again. Last ride wasn't even over yet.	2021-12-15 06:20:09
@d0nutptr	On CVE-2021-45046 twitter.com/d0nutptr/statu…	2021-12-15 06:20:13
@hhariri	Another day. Another vulnerability. lunasec.io/docs/blog/log4…	2021-12-15 06:20:31
@maxitehnicus	lunasec.io/docs/blog/log4… #log4j part 2	2021-12-15 06:23:19
@updates_hindi	■■■■■ Log4j ■■■■■■■■ (CVE-2021-45046) ■■■■■ ■■■■ _ ■■■■ ■■■■ ■■■■■ ■■■■■ ■■■■ hinditechupdates.tech/second-log4j-v…	2021-12-15 06:23:41
@Vigil8_DatSec	Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released bit.ly/3DUqWlr https://t.co/lwFwOZtVqG	2021-12-15 06:26:22
@pmf	Aw, shucks: > Our research into this shows that this new CVE invalidates previous mitigations lunasec.io/docs/blog/log4…	2021-12-15 06:27:01
@YUSUPHKILEO	#Infosec UPDATE: @TheASF has issued a new patch (CVE-2021-45046) for #Log4j utility. The previous patch for the… twitter.com/i/web/status/1…	2021-12-15 06:27:13
@DanWeb2_0	Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released bit.ly/3E9r33b noreply@blogger.com (Ravie Lakshmanan)	2021-12-15 06:30:05
@HighSNHN	Log4Shell update: second Log4j vulnerability published: lunasec.io/docs/blog/log4… (news.ycombinator.com/item?id=295615…)	2021-12-15 06:30:27
@JinibaBD	⚠ Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released #DataBreaches #DarkWeb #CyberSec… twitter.com/i/web/status/1…	2021-12-15 06:32:24
@AntiVirusLV	#Apache Foundation has issued a new patch (CVE-2021-45046) for #Log4j utility after the previous patch for the rece… twitter.com/i/web/status/1…	2021-12-15 06:34:29
@spiegel_2007	Log4j 2.16.0 で修正された脆弱性には CVE-2021-45046 のIDが振られている logging.apache.org/log4j/2.x/secu…	2021-12-15 06:39:25
@cyberethical_me	Log4shell 2.0 update: #log4shell #log4j #CyberSecurity	2021-12-15 06:40:39

@ohhara_shiojiri	「任意のコード実行の脆弱性（CVE-2021-44228）への対策に加え、サービス運用妨害攻撃の脆弱性（CVE-2021-45046）などのリスクに対応するため、2.16.0または2.12.2へのアップデートを推奨します。」	2021-12-15 06:41:49
@MichelGuillout	Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released thehackernews.com/2021/12/second… via @TheHackersNews	2021-12-15 06:43:01
@mgembejr	Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released thehackernews.com/2021/12/second… via @TheHackersNews	2021-12-15 06:51:31
@hasanfd	hatayi duzeltirken baska bir guvenlik acigina sebep verilmis anlasilan.. oncall olmak icin kotu zamanlar lunasec.io/docs/blog/log4…	2021-12-15 06:53:38
@marcosDLCS	lunasec.io/docs/blog/log4…	2021-12-15 06:54:36
@tsukamoto	メモ。Apache Log4j 2.15.0のCVE-2021-44228対応修正が不完全だったとして、CVE-2021-45046が登録され、Log4j 2.16.0がリリースされている。… twitter.com/i/web/status/1…	2021-12-15 06:57:33
@nl_Tazzy	@DeleriousMadman @T3ssalati0n @UK_Daniel_Card Waking up with sucks...	2021-12-15 06:58:15
@LaetitiaPayombo	Second #Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released thehackernews.com/2021/12/second…	2021-12-15 06:58:18
@marcodavids	Bummer...! #log4j #log4j2	2021-12-15 07:58:24
@jverhoelen	Let's dive into the next round of #log4j patching! The fix from 2.15.0 yields new CVE-2021-45046 because it was inc… twitter.com/i/web/status/1…	2021-12-15 08:01:09
@newsyc250	Log4Shell update: second Log4j vulnerability published lunasec.io/docs/blog/log4… (news.ycombinator.com/item?id=295615…)	2021-12-15 08:03:26
@tecnicahack	Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released dlvr.it/SFPTlh https://t.co/a7ZXj3xZuP	2021-12-15 08:04:04
@ipssignatures	The vuln CVE-2021-45046 has a tweet created 0 days ago and retweeted 13 times. twitter.com/HackerGautam/s… #pow1rtrtwwcve	2021-12-15 08:06:01
@spletinc	@Minecraft are the security fix versions also safe against the new version of log4shell? lunasec.io/docs/blog/log4…	2021-12-15 08:06:32
@ScinaryCyber	Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released dlvr.it/SFPVQ2 https://t.co/Yrdre2B3Xm	2021-12-15 08:08:33
@MoartnW	Argh CVE-2021-45046	2021-12-15 08:12:16
@nubeblog	Log4Shell Update: Second log4j Vulnerability Published (CVE-2021-44228 + CVE-2021-45046) | LunaSec lunasec.io/docs/blog/log4…	2021-12-15 08:12:56
@Securityblog	Log4Shell Update: Second log4j Vulnerability Published (CVE-2021-44228 + CVE-2021-45046) | LunaSec lunasec.io/docs/blog/log4…	2021-12-15 08:16:15
@YorickReintjens	Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released thehackernews.com/2021/12/second… #log4j #CyberSecurity	2021-12-15 08:17:03
@AlisherkaAlimov	somebody pls stop research bugs in log4j. just migrated to 2.15 and this again	2021-12-15 08:22:17
@beingsheerazali	Security Analysis of the 2nd Log4j CVE published earlier (CVE-2021-45046 / Log4Shell2) lunasec.io/docs/blog/log4…… twitter.com/i/web/status/1…	2021-12-15 08:26:42
@nerubesa	CVE - CVE-2021-45046 ift.tt/3F0iQ2k	2021-12-15 08:29:13
@dailydotdevhi	@TheHackersNews your article “Second Log4j Vulnerability (CVE-2021-45046) Discovered	2021-12-15

	— New Patch Released” was view… twitter.com/i/web/status/1…	08:30:03
@HackerMonks	URGENT: Apache Foundation has issued a new patch (CVE-2021-45046) for Log4j utility after the previous patch for th… twitter.com/i/web/status/1…	2021-12-15 09:15:25
@edgescan	CVE Record - fix for #log4j is incomplete. Check your efforts to date. cve.org/CVERecord?id=C…	2021-12-15 09:19:21
@CyberDonkyx0	#Log4j - CVE-2021-45046 It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete i… twitter.com/i/web/status/1…	2021-12-15 09:19:24
@huphu	Second log4j Vulnerability Published - lunasec.io/docs/blog/log4…	2021-12-15 09:21:04
@_orcaman	- למי שחוגג, יש אפטר פארטי: lunasec.io/docs/blog/log4… - לא, אין לנו קוד ג׳אווה (אני לא שונא אף שפה בעיקרון אבל כן שונ… twitter.com/i/web/status/1…	2021-12-15 09:21:16
@digeex_security	Log4Shell Update: Second log4j Vulnerability Published (CVE-2021-44228 + CVE-2021-45046) | LunaSec: lunasec.io/docs/blog/log4…	2021-12-15 09:21:21
@mame82	... mit dem Booster-Patch für CVE-2021-45046 dann auch mindestens 4 Wochen warten. #log4j twitter.com/DaRenegader/st…	2021-12-15 09:24:55
@sarmentots	Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released thehackernews.com/2021/12/second… via @TheHackersNews	2021-12-15 09:29:23
@tony_cleal	Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released thehackernews.com/2021/12/second… via @TheHackersNews	2021-12-15 09:30:30
@domineefh	Log4Shell Update: Second #log4j Vulnerability Published (CVE-2021-44228 + CVE-2021-45046) | LunaSec… twitter.com/i/web/status/1…	2021-12-15 09:31:09
@SimonByte	Heads up: Log4Shell update: second log4j vulnerability published CVE-2021-45046: the fix to address CVE-2021-4422… twitter.com/i/web/status/1…	2021-12-15 09:43:25
@Jangari_nTK	CVE-2021-45046 を考慮して KB の回避策が更新されるかもって書いてあるなぁ（遠い目 core.vmware.com/vmsa-2021-0028…	2021-12-15 09:43:35
@CelerityLimited	Second #Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released bit.ly/3273udC by… twitter.com/i/web/status/1…	2021-12-15 09:45:51
@HackEast1	#عاجل أصدرت Apache ترقيع جديدً (CVE-2021-45046) للأداة المساعدة #log4j بعد أن تم اعتبار الترقيع السابق لاستغلال… twitter.com/i/web/status/1…	2021-12-15 09:47:36
@ciberconsejo	Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released thehackernews.com/2021/12/second… vía @TheHackersNews	2021-12-15 09:51:34
@uproditnetwork	Since the CVE CVE-2021-45046, we're upgrading again log4j2 implementation of slf4j. Sorry for the downtime… twitter.com/i/web/status/1…	2021-12-15 09:51:51
@mushroom080	えまってCVE-2021-45046？？？キャッチおくれた	2021-12-15 09:55:04
@floriantraun	...so, one #Log4j #vulnerability wasn't enough, we got a second one now to take care of? lunasec.io/docs/blog/log4…… twitter.com/i/web/status/1…	2021-12-15 09:56:29
@steveburnley	Apache Log4j 2 Security Vulnerability CVE-2021-45046 - Kronos hit with ransomware, warns of data breach and 'severa… twitter.com/i/web/status/1…	2021-12-15 09:57:36
@mushroom080	CVE - CVE-2021-45046	2021-12-15 09:57:44
@sjuerges	@3811015 Äh, jetzt leider schon. CVE-2021-45046 ?	2021-12-15 09:59:06
@jedisct1	Log4Shell Update: Second log4j Vulnerability Published (CVE-2021-44228 + CVE-2021-45046) lunasec.io/docs/blog/log4…	2021-12-15 10:03:09
@mendelson	mendelson AS2 2021 b533 released Fix for the Log4j security problem (CVE-2021-45046)	2021-12-15

	More at: mendelson-e-c.com/node/27357	10:04:43
@mendelson	mendelson OFTP2 2021 b328 released Fix for the Log4j security problem (CVE-2021-45046) More at: mendelson-e-c.com/node/27358	2021-12-15 10:05:54
@ipssignatures	The vuln CVE-2021-45046 has a tweet created 0 days ago and retweeted 120 times. twitter.com/TheHackersNews… #pow2rtrtwwcve	2021-12-15 10:06:00
@TacticalGrace	@matiwinnetou CVE-2021-45046 talks about “certain non-default configurations”. So it can be good for you, but still… twitter.com/i/web/status/1…	2021-12-15 10:06:28
@dnsmichi	Log4Shell Update: Second #log4j Vulnerability Published (CVE-2021-44228 + CVE-2021-45046) | LunaSec buff.ly/3s8FAK6	2021-12-15 10:57:07
@WyriHaximus	@gnuconsulting @dogmatic69 Also, reset the clock a new one has been found: lunasec.io/docs/blog/log4…	2021-12-15 11:00:35
@WebOjos	After #log4shell #CVE-2021-44228, One more flaw #CVE-2021-45046 is expecting a patch.	2021-12-15 11:06:13
@richardfan1126	@SumoLogic_Help @SumoLogic My question is: does CVE-2021-45046 impact Sumo Collector 19.361-12	2021-12-15 11:07:11
@mendelson	mendelson converterIDE 2020 b290 released Fix for the Log4j security problem (CVE-2021-45046) More at: mendelson-e-c.com/node/27360	2021-12-15 11:09:02
@_Blackmac	Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released thehackernews.com/2021/12/second…	2021-12-15 11:17:39
@AlaaAttya	common! lunasec.io/docs/blog/log4…	2021-12-15 11:17:42
@noisymouse27f	FFS, a second one for log4j2?	2021-12-15 11:17:54
@vojtechmares_	Oh shit, here we go again... Second vulnerability in log4j... #CVE CVE-2021-45046 twitter.com/dnsmichi/statu…	2021-12-15 11:19:38
@dailydotdevhi	@TheHackersNews You just got 500 views for “Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Rele… twitter.com/i/web/status/1…	2021-12-15 11:20:03
@jn66data	See the latest cyber and data science articles! Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patc… twitter.com/i/web/status/1…	2021-12-15 11:20:37
@spotter	O kurka, idziemy znów. cve.org/CVERecord?id=C…	2021-12-15 11:21:15
@IT_news_for_all	Больше уязвимостей в log4j богу уязвимостей! lunasec.io/docs/blog/log4…... t.me/s/it_news_for_… https://t.co/Nsze8onwR9	2021-12-15 11:25:08
@MattCASmith	Second #Log4Shell vulnerability gets attackers past previous workarounds (but is still fixed by patching). #infosec lunasec.io/docs/blog/log4…	2021-12-15 11:30:13
@spotmac	I suspect Jamf Pro is still vulnerable. Version 2.15.0 was used in the 10.31.1 update. CVE-2021-45046 a workaround… twitter.com/i/web/status/1…	2021-12-15 11:30:36
@RonaldsVilcins	Log4Shell Update: Second log4j Vulnerability Published (CVE-2021-44228 + CVE-2021-45046) lunasec.io/docs/blog/log4…	2021-12-15 11:30:54
@ThisIsWhyICode	Log4Shell round 2 #programming	2021-12-15 11:42:21
@alim_zhan	Больше уязвимостей в log4j богу уязвимостей! lunasec.io/docs/blog/log4… https://t.co/qNpLeCkIa3	2021-12-15 11:42:34
@programemes	log4j2 developers talking about log2shell mitigation and introduce then CVE-2021-45046 Source:… twitter.com/i/web/status/1…	2021-12-15 12:34:03
@neverping	Meanwhile: lunasec.io/docs/blog/log4…	2021-12-15

		12:36:48
@pilar_shmeelar	Dear god lunasec.io/docs/blog/log4… #log4j #infosecurity	2021-12-15 12:48:28
@nicolaferrini	Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released thehackernews.com/2021/12/second… https://t.co/2BStb0YZGr	2021-12-15 12:48:36
@JensGleichmann	Some updates on the #log4j topic: - included details of CVE-2021-45046 - added details for BTP Cloud Foundry applic… twitter.com/i/web/status/1…	2021-12-15 12:55:30
@axcheron	Second Log4j Vulnerability (CVE-2021-45046) Discovered thehackernews.com/2021/12/second… #Log4j	2021-12-15 12:55:41
@jpcarsi	?Apache Foundation publicó un nuevo parche (CVE-2021-45046) para #Log4j después de que el parche anterior para el e… twitter.com/i/web/status/1…	2021-12-15 12:58:03
@yeroncio	Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released thehackernews.com/2021/12/second… a través de @TheHackersNews	2021-12-15 12:58:36
@minamijoyo	“Log4Shell Update: Second log4j Vulnerability Published (CVE-2021-44228 + CVE-2021-45046)	LunaSec” htn.to/33pazwLupH	2021-12-15 12:58:55
@jbhall56	Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released thehackernews.com/2021/12/second… via @TheHackersNews	2021-12-15 13:02:15
@oss_security	Re: CVE-2021-45046: Apache Log4j2 Thread Context Message Pattern and Context Lookup Pattern vulnerable to a denial… twitter.com/i/web/status/1…	2021-12-15 13:02:32
@reddit_progr	Log4Shell Update: Second log4j Vulnerability Published (CVE-2021-44228 + CVE-2021-45046)	LunaSec… twitter.com/i/web/status/1…	2021-12-15 13:14:22
@Imosphere	UPDATE 15/12: A 2nd vulnerability has been announced, CVE-2021-45046. We can confirm our products are not affected… twitter.com/i/web/status/1…	2021-12-15 13:17:00
@southerncyber	TalosSecurity: We've updated our #Log4J blog post to cover the newly discovered CVE-2021-45046 that's been identifi… twitter.com/i/web/status/1…	2021-12-15 14:26:41
@hostifi_net	We're working on updating all of our servers to #UniFi Network version 6.5.55 today to patch CVE-2021-45046. This… twitter.com/i/web/status/1…	2021-12-15 14:30:49
@TaylorParizo	CVE-2021-45046, CVE-2021-43890, and Log4Shell attribution aren't helping. twitter.com/sshell_/status…	2021-12-15 14:31:27
@SharjeelSayed	lunasec.io/docs/blog/log4… lunasec.io/docs/blog/log4…	2021-12-15 14:33:06
@silveira	Já ajeitou seu Log4j? Poisé, já tem outra vulnerabilidade. lunasec.io/docs/blog/log4…	2021-12-15 14:33:41
@w0mbat5eoul	CVE-2021-45046 has been given a CVSS Base Score of 3.7 logging.apache.org/log4j/2.x/secu… https://t.co/zjfycrhEL9	2021-12-15 14:36:31
@NewRelicJapan	CVE-2021-44228 に加えてCVE-2021-45046 まで含めたNew Relicにおける取り組みとお客様にお願いしたい対応について本社記事を抄訳しました	Apache Log4j の脆弱性に関連する New… twitter.com/i/web/status/1…	2021-12-15 14:37:40
@MCaraggiu	This was reported as CVE-2021-45046 on December 14. Following the disclosure of this vulnerability, a new version o… twitter.com/i/web/status/1…	2021-12-15 14:38:03
@ohhara_shiojiri	Protection against CVE-2021-45046, the additional Log4j RCE vulnerability blog.cloudflare.com/protection-aga…	2021-12-15 14:40:49
@d4nys3k	@NUKIB_CZ @Lupacz Chtelo by to rozsirit, fix CVE-2021-44228 nestaci... mame tu nove CVE-2021-45046... threatpost.com/apache-patch-l…	2021-12-15 14:42:37
@TiitHallas	Patched the #log4j vulnerability from last friday? Good boy. And now once more! lunasec.io/docs/blog/log4… #logshell #patch #Security	2021-12-15 14:54:16

@libertarianmar5	lunasec.io/docs/blog/log4…	2021-12-15 14:55:28
@SqlWorldWide	@ArmorDba #sqlhelp CVE-2021-45046 Log4j 1.x mitigation: Log4j 1.x is not impacted by this vulnerability.	2021-12-15 15:59:14
@MnkeniFrancis	Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released #Cybersecurity #security via… twitter.com/i/web/status/1…	2021-12-15 15:59:20
@peterpan2000355	Security Vulnerability CVE-2021-45046 The Log4j team has been made aware of a security vulnerability, CVE-2021-4504… twitter.com/i/web/status/1…	2021-12-15 16:04:35
@SecludIT	Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released thehackernews.com/2021/12/second… via @TheHackersNews	2021-12-15 16:07:22
@getsecureworld	Here we go again ... a new version of the log4j vulnerability ... CVE-2021-45046 ... until now the exploitation of… twitter.com/i/web/status/1…	2021-12-15 16:11:40
@trip_elix	"RT @TheHackersNews: URGENT: Apache Foundation has issued a new patch (CVE-2021-45046) for #Log4j utility after the… twitter.com/i/web/status/1…	2021-12-15 16:12:44
@wheresrhys	@neo4j @mesirii A new vulnerability in the patched log4j has been found . Are you actively w… twitter.com/i/web/status/1…	2021-12-15 16:14:14
@_Blackmac	CVE-2021-45046 ??♂	2021-12-15 16:18:19
@hajaveeb	Kahjuks tsirkus käib edasi ja aina lõbusamaks läheb (veidi pätšimatu auk ja lisaaugud) lunasec.io/docs/blog/log4… twitter.com/ronaldliive/st…	2021-12-15 16:19:46
@kenhuangus	Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released thehackernews.com/2021/12/second… 来自 @TheHackersNews	2021-12-15 16:19:49
@geko_cloud	Algunas configuraciones non-default en log4j 2.15.0 permiten un ataque de DoS: #ops #log4j #log4shell #cve	2021-12-15 16:24:18
@cooked_go9ma	log4j JDNILookup makes Dos Attack action CVE-2021-45046	2021-12-15 16:28:50
@SecRecon	CVE - CVE-2021-45046: It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in… twitter.com/i/web/status/1…	2021-12-15 16:32:14
@RProgramming150	Log4Shell Update: Second log4j Vulnerability Published (CVE-2021-44228 + CVE-2021-45046) | LunaSec… twitter.com/i/web/status/1…	2021-12-15 16:33:52
@MarionaJava	Parece que con pasar a 2.15.0 no era suficiente, han encontrado otra: CVE-2021-45046: hay que poner la versión de log4j-core a 2.16.0.	2021-12-15 16:37:53
@Nihilisme10	My new fav tweet: URGENT: Apache Foundation has issued a new patch (CVE-2021-45046) for #Log4j utility after the p… twitter.com/i/web/status/1…	2021-12-15 17:50:49
@elhackernet	Una segunda vulnerabilidad Log4Shell ▶ log4j (CVE-2021-44228 + CVE-2021-45046) lunasec.io/docs/blog/log4…	2021-12-15 17:55:53
@SCALEtruecharts	**More log4j patches** Due to CVE-2021-45046 we will do another round of additional container updates.	2021-12-15 17:56:15
@veronicabp_	#Vulnerabilidad #log4j para la versión 2.15	2021-12-15 17:59:44
@zephel01	Protection against CVE-2021-45046, the additional Log4j RCE vulnerability blog.cloudflare.com/protection-aga…	2021-12-15 17:59:52
@RProgramming200	Log4Shell Update: Second log4j Vulnerability Published (CVE-2021-44228 + CVE-2021-45046) | LunaSec… twitter.com/i/web/status/1…	2021-12-15 18:06:00
@ipssignatures	The vuln CVE-2021-45046 has a tweet created 0 days ago and retweeted 14 times. twitter.com/Cloudflare/sta… #pow1rtrtwwcve	2021-12-15 18:06:01

@ipssignatures	The vuln CVE-2021-45046 has a tweet created 0 days ago and retweeted 12 times. twitter.com/FilipiPires/st… #pow1rtrtwwcve	2021-12-15 18:06:02
@sergeykandaurov	Done updating log4j to 2.15.0 everywhere? Time to update to 2.16.0! blog.cloudflare.com/protection-aga…	2021-12-15 18:13:36
@bandersnatchist	Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released thehackernews.com/2021/12/second… @TheHackersNewsより	2021-12-15 18:18:16
/r/netcve	CVE-2021-45046	2021-12-14 17:38:08
/r/vulnintel	Incomplete fix for CVE-2021-44228 (log4shell) causes a DOS vulnerability in Apache Log4j 2.15.0 CVE-2021-45046	2021-12-14 20:57:23
/r/sysadmin	New Log4J CVE	2021-12-14 20:27:31
/r/programming	Analysis of the 2nd Log4j CVE published earlier (CVE-2021-45046 / Log4Shell2)	2021-12-15 04:00:19
/r/cybersecurity	Security Analysis of the 2nd Log4j CVE published earlier (CVE-2021-45046 / Log4Shell2)	2021-12-15 03:48:53
/r/netsec	Security Analysis of the 2nd Log4j CVE published earlier (CVE-2021-45046 / Log4Shell2)	2021-12-15 03:44:26
/r/hacking	Log4Shell Update: Second log4j Vulnerability Published (CVE-2021-44228 + CVE-2021-45046) | LunaSec	2021-12-15 07:23:40
/r/programming	Log4Shell Update: Second log4j Vulnerability Published (CVE-2021-44228 + CVE-2021-45046) | LunaSec	2021-12-15 07:15:41
/r/hacking	Second log4j Vulnerability Published (CVE-2021-44228 + CVE-2021-45046)	2021-12-15 10:02:29
/r/unifi_versions	UniFi Network Application 6.5.55	2021-12-15 09:35:08
/r/CyberNews	Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released	2021-12-15 11:03:38
/r/CloudFlare	Protection against CVE-2021-45046, the additional Log4j RCE vulnerability	2021-12-15 14:20:06
/r/sysadmin	Mitigating log4j in Windows?	2021-12-15 15:52:35
/r/devopsish	Log4Shell Update: Second log4j Vulnerability Published (CVE-2021-44228 + CVE-2021-45046) | LunaSec	2021-12-15 17:05:31
/r/RedSec	Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released	2021-12-15 18:01:28
/r/cybersecurity	Responding to CVE-2021-45046	2021-12-15 23:58:55
/r/newsokuexp	JavaのLog4jライブラリで「Log4Shell」に加えて新たな脆弱性「CVE-2021-45046」が発覚、アップデートで対応可能	2021-12-16 05:36:37
/r/SecOpsDaily	Protection against CVE-2021-45046, the additional Log4j RCE vulnerability	2021-12-16 10:23:56
/r/Rundeck	Rundeck 3.4.8 release	2021-12-16 16:40:44
/r/devopsish	Understanding Log4Shell via Exploitation and Live Patching (CVE-2021-44228 + CVE-2021-45046) | LunaSec	2021-12-16 17:37:09

/r/programming	Log4Shell Update: Severity Upgraded 3.7 -> 9.0 for Second log4j Vulnerability (CVE-2021-45046)	2021-12-17 11:16:41
/r/TPLink_Omada	Omada v4/v5 updates for Linux and Windows now available with Log4Shell fixes	2021-12-17 12:16:33
/r/sysadmin	CVE-2021-45046 (Log4j vulnerability #2) upgraded to CVSS 9.0	2021-12-17 15:01:12
/r/sysadmin	Log4Shell Update: Severity Upgraded 3.7 -> 9.0 for Second log4j Vulnerability (CVE-2021-45046)	2021-12-17 16:34:48
/r/blueteamsec	Log4Shell Update: Severity Upgraded 3.7 -> 9.0 for Second log4j Vulnerability (CVE-2021-45046) | LunaSec - v2.15 of Log4j has an RCE	2021-12-17 15:46:42
/r/minecraftclients	log4j exploit	2021-12-17 20:34:51
/r/sysadmin	Log4jSherlock a fast PowerShell script that can scan multiple computers, made by a paranoid sysadmin.	2021-12-20 00:45:19
/r/programming	Log4j Vulnerability CVE-2021-45105: What You Need to Know (and how it differs from CVE-2021-45046)	2021-12-20 07:33:15
/r/netsec	Log4j Vulnerability CVE-2021-45105: What You Need to Know (and how it differs from CVE-2021-45046)	2021-12-20 07:32:40
/r/selfhosted	Log4j2 nightmares for self hosters?	2021-12-21 16:54:56
/r/bag_o_news	Log4j Vulnerability CVE-2021-45105: What You Need to Know (and how it differs from CVE-2021-45046)	2021-12-21 18:04:50
/r/vulnintel	Mitigating Log4Shell and Other Log4j-Related Vulnerabilities CVE-2021-44228 CVE-2021-45046 CVE-2021-45105	2021-12-23 10:14:43
/r/arlo	Log4j vulnerability	2021-12-23 13:08:29
/r/u/stellarcyber	Stellar Cyber: Log4j Vulnerability and Exploitation Detection	2022-01-08 13:39:36
/r/TPLink_Omada	Omada Controller OC200 update received today	2022-01-08 13:18:14
/r/sysadmin	FedEx Ship Manager still has Log4j vulnerability after update.	2022-01-11 00:14:00
/r/msp	VMware Horizon servers being actively hit with Cobalt Strike	2022-01-15 01:39:18
/r/blueteamsec	Log4j CVE-2021-44228 and CVE-2021-45046 in VMware Horizon and VMware Horizon Agent (on-premises) (87073)	2022-01-16 09:38:49
/r/Security_News	Second Log4j Vulnerability (CVE-2021-45046) Discovered — New Patch Released The Apache Software program Basis (ASF)...	2022-01-18 23:52:28
/r/u/detoxtechnologie	What Is Log4Shell? The Log4j Vulnerability Explained in 2022	2022-01-25 05:25:17
/r/vmware	IMPORTANT: Log4j CVE-2021-44228 and CVE-2021-45046 in VMware Horizon and VMware Horizon Agent (on-premises) (87073)	2022-01-25 23:32:13
/r/throwaway_the_videos	Fuzzing Java to Find Log4j Vulnerability - CVE-2021-45046 — LiveOverflow	2022-02-01 16:55:28
/r/PFSENSE	help: Suricata shuts down after several minutes	2022-04-09 16:21:29

/r/u/Master_Rip_3449	Analysis of the 2nd Log4j CVE published earlier (CVE-2021-45046 / Log4Shell2)	2022-08-26 01:53:28
/r/learnpython	shamefully but i need help to finish my work..pleas help me	2022-11-09 18:50:16

← Previous ID

Next ID→