Advisory Alert

Alert Number: AAA20211221 **Date:** December 21, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Multiple Products	Critical	Multiple Vulnerabilities

Description

Affected Product	**Multiple Products**
Severity	**Critical**
Affected Vulnerability	**Multiple Vulnerabilities (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-4104)**
Description	CVE-2021-44228 - An unauthenticated, remote attacker could exploit this flaw by sending a specially crafted request to a server running a vulnerable version of log4j. The specially crafted request uses a Java Naming and Directory Interface (JNDI) injection via Lightweight Directory Access Protocol (LDAP), Secure LDAP (LDAPS), Remote Method Invocation (RMI), Domain Name Service (DNS). Successful exploitation of this Vulnerability could allow a remote attacker to execute arbitrary code and lead to gain full control of the targeted servers. CVE-2021-45046 - Apache Log4j is vulnerable to a denial of service, caused by an incomplete fix of CVE-2021-44228 in certain non-default configurations. A remote attacker with control over Thread Context Map (MDC) input data or a Thread Context Map pattern to exploit this vulnerability to craft malicious input data using a JNDI Lookup pattern and cause a denial of service. CVE-2021-45105 - Apache Log4j2 versions 2.0-alpha1 through 2.16.0 (excluding 2.12.3) did not protect from uncontrolled recursion from self-referential lookups. This allows an attacker with control over Thread Context Map data to cause a denial of service when a crafted string is interpreted CVE-2021-4104 - Apache Log4j could allow a remote attacker to execute arbitrary code on the system, caused by the deserialization of untrusted data when the attacker has write access to the Log4j configuration. If the deployed application is configured to use JMSAppender, an attacker could exploit this vulnerability to execute arbitrary code on the system. The vulnerability has been exploited in the wild, Users are highly recommended to update to the latest version to mitigate the risk associated with the flaws.

Affected Products

Juniper Juniper Networks Cross Provisioning Platform Juniper Networks Juniper Secure Analytics Risk Manager Juniper Networks Network and Security Manager (NSM) Juniper Networks WANDL IP/MPLSView Juniper Networks BTI proNX Service Manager Software Juniper Networks JSA Series User Behavior Analytics Juniper Networks Junos Space Network Management Platform when OpenNMS has been enabled. Juniper Networks NorthStar Controller / NorthStar Planner Juniper Networks Paragon Pathfinder Juniper Networks Paragon Planne	**Cisco** Collaboration and Social Media Endpoint Clients and Client Software Network Application, Service, and Acceleration Network and Content Security Devices Network Management and Provisioning Routing and Switching - Enterprise and Service Provider Unified Computing Voice and Unified Communications Devices Video, Streaming, TelePresence, and Transcoding Devices Wireless
INTEL Intel Audio Development Kit Intel Datacenter Manager Intel oneAPI sample browser plugin for Eclipse Intel System Debugger Intel Secure Device Onboard Intel Genomics Kernel Library Intel System Studio Computer Vision Annotation Tool maintained by Intel Intel Sensor Solution Firmware Development Kit	**Fortinet** FortiAIOps FortiCASB FortiConverter Portal FortiCWP FortiEDR Cloud FortiInsight FortiIsolator FortiMonitor FortiPortal FortiSIEM ShieldX
DELL Multiple Products	**HP** Multiple Products
Oracle Java SE Version Prior to 6u212 Java SE Version Prior to 7u202 Java SE Version Prior to 8u192 Java SE Version Prior to 11.0.2	**IBM** WebSphere Application Server IBM Security Guardium IBM Spectrum Protect Backup-Archive Client and IBM Spectrum Protect for Virtual Environments IBM Tivoli Monitoring IBM Spectrum Copy Data Management IBM QRadar SIEM
PaloAlto PAN-OS for Panorama Exact Data Matching CLI	**RedHat** Red Hat OpenShift Container Platform 4.6, 4.7, 4.8 OpenShift Logging 5.0, 5.1, 5.2, 5.3 Red Hat JBoss Enterprise Application Platform 7 Red Hat Process Automation 7 Red Hat AMQ Streams 1 Red Hat CodeReady Studio 12 Red Hat Integration Camel K Red Hat Integration Camel Quarkus Red Hat JBoss Fuse 7 Red Hat OpenShift Application Runtimes 1.0 Red Hat AMQ Streams 1
VMware VMware Horizon VMware vCenter Server VMware HCX VMware NSX-T Data Center VMware Unified Access Gateway VMware WorkspaceOne Access	**Citrix** Citrix Endpoint Management (Citrix XenMobile Server) Citrix Virtual Apps and Desktops (XenApp & XenDesktop)

	VMware Identity Manager VMware vRealize Operations VMware vRealize Operations Cloud Proxy VMware vRealize Automation VMware vRealize Lifecycle Manager VMware Site Recovery Manager, vSphere Replication VMware Carbon Black Cloud Workload Appliance VMware Carbon Black EDR Server VMware Tanzu GemFire VMware Tanzu GemFire for VMs VMware Tanzu Greenplum VMware Tanzu Operations Manager VMware Tanzu Application Service for VMs VMware Tanzu Kubernetes Grid Integrated Edition VMware Tanzu Observability by Wavefront Nozzle Healthwatch for Tanzu Application Service Spring Cloud Services for VMware Tanzu Spring Cloud Gateway for VMware Tanzu Spring Cloud Gateway for Kubernetes API Portal for VMware Tanzu Single Sign-On for VMware Tanzu Application Service App Metrics VMware vCenter Cloud Gateway VMware vRealize Orchestrator VMware Cloud Foundation VMware Workspace ONE Access Connector VMware Horizon DaaS VMware Horizon Cloud Connector VMware NSX Data Center for vSphere VMware AppDefense Appliance VMware Cloud Director Object Storage Extension VMware Telco Cloud Operations VMware vRealize Log Insight VMware Tanzu Scheduler VMware Smart Assurance NCM VMware Smart Assurance SAM [Service Assurance Manager] VMware Integrated OpenStack VMware vRealize Business for Cloud VMware vRealize Network Insight VMware Cloud Provider Lifecycle Manager VMware SD-WAN VCO VMware NSX-T Intelligence Appliance	**Sonicwall** Soniwall Email Security Soniwall NSM Soniwall WAF

Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	**Fortinet** https://www.fortiguard.com/psirt/FG-IR-21-245 **Juniper** https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11259&cat=SIRT_1&actp=LIST **Cisco** https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd **Oracle** https://www.oracle.com/security-alerts/alert-cve-2021-44228.html **PaloAlto** https://security.paloaltonetworks.com/CVE-2021-44228 **IBM** https://www.ibm.com/support/pages/node/6527082 https://www.ibm.com/support/pages/node/6527080 https://www.ibm.com/support/pages/node/6527962 https://www.ibm.com/support/pages/node/6527830

https://www.ibm.com/support/pages/node/6526640
https://www.ibm.com/support/pages/node/6526750

DELL
https://www.dell.com/support/kbdoc/en-us/000194414/dell-response-to-apache-log4j-remote-code-execution-vulnerability
https://www.dell.com/support/kbdoc/en-us/000194544/dsa-2021-287-dell-emc-srs-policy-manager-security-update-for-apache-log4j-remote-code-execution-vulnerability-cve-2021-44228
https://www.dell.com/support/kbdoc/en-us/000194503/dsa-2021-274-dell-emc-data-domain-security-update-for-apache-log4j-remote-code-execution-vulnerability-cve-2021-44228
https://www.dell.com/support/kbdoc/en-us/000194466/dsa-2021-265-dell-emc-vxrail-security-update-for-apache-log4j-remote-code-execution-vulnerability-cve-2021-44228
https://www.dell.com/support/kbdoc/en-us/000194416/additional-information-for-apache-log4j-remote-code-execution-vulnerability-cve-2021-44228
https://www.dell.com/support/kbdoc/en-us/000194541/dsa-2021-280-dell-emc-networker-security-update-for-apache-log4j-remote-code-execution-vulnerability-cve-2021-44228
https://www.dell.com/support/kbdoc/en-us/000194630/dsa-2021
https://www.dell.com/support/kbdoc/en-us/000194627/dsa-2021-297-dell-emc-streaming-data-platform-security-update-for-apache-log4j-remote-code-execution-vulnerability-cve-2021-44228-cve-2021-45046
https://www.dell.com/support/kbdoc/en-us/000194638/dsa-2021-275-dell-emc-openmanage-enterprise-security-update-for-apache-log4j-remote-code-execution-vulnerability-cve-2021-44228

INTEL
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00646.html

HP
https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04215en_us

RedHat
https://access.redhat.com/security/cve/CVE-2021-44228

Citrix
https://support.citrix.com/article/CTX335705

VMware
https://www.vmware.com/security/advisories/VMSA-2021-0028.html

Sonicwall
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0032

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.