Article Number: 000194414

Print

Dell Response to Apache Log4j Remote Code Execution Vulnerability

Summary: On December 10, 2021, a critical remote code vulnerability was published concerning the Apache Log4j library. Dell is in the process of assessing potential impact to its products.

Audience Level: Customer

Article Content

Security Article Type

Security KB

CVE Identifier

CVE-2021-44228

Issue Summary

Apache Publication: Apache Log4j Remote Code Execution

CVE Details: CVE-2021-44228

Details

Dell is reviewing the recently published Apache Log4j Remote Code Execution vulnerability being tracked in CVE-2021-44228 and assessing impact on our products. The security of our products is a top priority and critical to protecting our customers.

Vulnerable Products

The following products are confirmed as impacted by the Apache Log4j vulnerability:

Product	Mitigation/Workaround	Security Update Release Timeline
APEX Console		Cloud environment patch in progress
APEX Data Storage Services		Cloud environment patch in progress
Cloud IQ		Cloud environment patch in progress
Connectrix (Cisco MDS DCNM)		TBD
Connectrix B-Series SANnav	See DSA-2021-266	
Data Domain OS	Workaround expected 12/15	
Dell EMC Avamar	See DSA-2021-277	

Dell EMC Cloud Disaster Recovery	Workaround expected 12/15	
Dell EMC Data Protection Central		TBD
Dell EMC Data Protection Search		TBD
Dell EMC ECS		Patch expected 12/17
Enterprise Hybrid Cloud		See DSA-2021-270
Dell EMC Enterprise Storage Analytics for vRealize Operations	See DSA-2021-278	
Dell EMC Integrated System for Microsoft Azure Stack Hub		TBD
Dell EMC NetWorker	Workaround expected 12/15	
Dell EMC NetWorker VE	TBD	
Dell EMC PowerFlex Appliance	Workaround expected 12/15	
Dell EMC PowerFlex Manager		TBD
Dell EMC PowerFlex Rack		TBD
Dell EMC PowerProtect Data Manager	Workaround expected 12/15	
Dell EMC PowerProtect DP Series Appliance (iDPA)	Workaround expected 12/15	
Dell EMC PowerStore		Patch expected 12/31
Dell EMC RecoverPoint		TBD
Dell EMC SRM vApp		TBD
Dell EMC Streaming Data Platform		TBD
Dell EMC Unity		Patch expected 12/31
Dell EMC Vplex		TBD
Dell EMC VxRail	See DSA-2021-265	
Dell Open Management Enterprise - Modular		Patch expected 12/17
DellEMC OpenManage Enterprise Services		Patch expected 12/17
OpenManage Enterprise		Patch expected 12/17
Dell EMC Ruckus SmartZone 300 Controller		TBD
Dell EMC Ruckus SmartZone 100 Controller		TBD
Dell EMC Ruckus Virtual Software		TBD

Secure Connect Gateway (SCG) 5.0 Appliance		TBD
SRS Policy Manager		TBD
SupportAssist Enterprise		TBD
Unisphere Central		TBD
Vblock		TBD
VNXe 1600		TBD
VNXe 3200		TBD
VxBlock		TBD
VxFlex Ready Nodes	Workaround expected 12/15	
vRealize Data Protection Extension		TBD
Wyse Management Suite		See DSA-2021-267

Products Confirmed Not Vulnerable

The following products are not impacted by the Apache Log4j vulnerability:

- Alienware Command Center
- Alienware OC Controls
- Alienware On Screen Display
- Alienware Update
- Atmos
- Azure Stack HCI
- CalMAN Powered Calibration Firmware
- CalMAN Ready for Dell
- Centera
- Chameleon Linux Based Diagnostics
- Chassis Management Controller (CMC)
- China HDD Deluxe
- Cloud Mobility for Dell EMC Storage
- Cloud Tiering Appliance
- Connectrix (Cisco MDS 9000 switches)
- Connextrix B Series
- CyberSense for PowerProtect Cyber Recovery
- CyberSecIQ Application
- Dell BSAFE Crypto-C Micro Edition
- Dell BSAFE Crypto-J
- Dell BSAFE Micro Edition Suite
- Dell Calibration Assistant
- Dell Cinema Color
- Dell Cloud Command Repository Manager
- Dell Cloud Management Agent
- Dell Color Management
- Dell Command Configure
- Dell Command Integration Suite for System Center
- Dell Command Intel vPro Out of Band
- Dell Command Monitor
- Dell Command Power Manager
- Dell Command PowerShell Provider
- Dell Command Update
- Dell EMC Container Storage Modules
- Dell Customer Connect
- Dell Data Guardian

- Dell Data Protection
- Dell Data Recovery Environment
- Dell Data Vault
- Dell Data Vault for Chrome OS
- Dell Deployment Agent
- Dell Digital Delivery
- Dell Direct USB Key
- Dell Display Manager 1.5 for Windows / macOS
- Dell Display Manager 2.0 for Windows / macOS
- Dell EMC AppSync
- Dell EMC Cloudboost
- Dell EMC CloudLink
- Dell EMC Data Computing Appliance (DCA)
- Dell EMC Data Protection Advisor
- Dell EMC DataIQ
- Dell EMC Disk Library for Mainframe
- Dell EMC GeoDrive
- Dell EMC Isilon InsightIQ
- Dell EMC License Manager
- Dell EMC Networking Onie
- Dell EMC OpenManage Ansible Modules
- Dell EMC OpenManage integration for Splunk
- Dell EMC OpenManage Integration for VMware vCenter
- Dell EMC OpenManage Management pack for vRealize Operations
- Dell EMC OpenManage Operations Connector for Micro Focus Operations Bridge Manager
- Dell EMC PowerMax and in market VMAX
- Dell EMC PowerPath
- Dell EMC PowerPath Management Appliance
- Dell EMC PowerProtect Cyber Recovery
- Dell EMC PowerScale OneFS
- Dell EMC PowerShell for PowerMax
- Dell EMC PowerShell for Powerstore
- Dell EMC PowerShell for Unity
- Dell EMC PowerSwitch Z9264F-ON BMC, Dell EMC PowerSwitch Z9432F-ON BMC
- Dell EMC Repository Manager (DRM)
- Dell EMC SourceOne
- Dell EMC Systems Update (DSU)
- Dell EMC Unisphere 360
- Dell EMC Virtual Storage Integrator
- Dell EMC XtremIO
- Dell Encryption Personal
- Dell Encryption Enterprise
- Dell Security Management Server and Dell Security Management Server Virtual
- Dell Endpoint Security Suite Enterprise
- Dell Hybrid Client
- Dell ImageAssist
- Dell Insights Client
- Dell Linux Assistant
- Dell Mobile Connect
- Dell Monitor ISP (Windows/Mac/Linux)
- Dell Monitor SDK
- Dell Networking X-Series
- Dell Open Manage Mobile
- Dell Open Manage Server Administrator
- Dell OpenManage Change Management
- Dell OpenManage Enterprise Power Manager Plugin
- Dell Optimizer
- Dell OS Recovery Tool
- Dell Peripheral Manager 1.4 / 1.5 for Windows
- Dell Platform Service
- Dell Power Manager

- Dell Power Manager Lite
- Dell Precision Optimizer
- Dell Precision Optimizer for Linux
- Dell Premier Color
- Dell Recovery (Linux)
- Dell Remediation Platform
- Dell Remote Execution Engine (DRONE)
- Dell Security Advisory Update - DSA-2021-088
- Dell SupportAssist SOS
- Dell Thin OS
- Dell Threat Defense
- Dell True Color
- Dell Trusted Device
- Dell Update
- Dream Catcher
- DUP Creation Service
- DUP Framework (ISG)
- Embedded NAS
- Embedded Service Enabler
- Fluid FS
- "iDRAC Service Module (iSM) "
- Infinity MLK (firmware)
- Integrated Dell Remote Access Controller (iDRAC)
- ISG Accelerators
- ISG Board & Electrical
- IsilonSD Management Server
- IVE-WinDiag
- Mainframe Enablers
- My Dell
- MyDell Mobile
- NetWorker Management Console
- Networking BIOS
- Networking DIAG
- Networking N-Series
- Networking OS 10
- Networking OS9
- Networking SD-WAN Edge SD-WAN
- Networking W-Series
- Networking X-Series
- OMIMSSC (OpenManage Integration for Microsoft System Center)
- OMIMSSC (OpenManage Integration for Microsoft System Center)
- OMNIA
- OMNIA
- OpenManage Connections - Nagios
- OpenManage Connections - ServiceNow
- OpenManage Integration for Microsoft System Center for System Center Operations Manager
- OpenManage Integration with Microsoft Windows Admin Center
- OpenManage Network Integration
- PowerConnect N3200
- PowerConnect PC2800
- PowerConnect PC8100
- PowerEdge BIOS
- PowerEdge Operating Systems
- PowerTools Agent
- PPDM Kubernetes cProxy
- PPDM VMware vProxy
- Redtail
- Remotely Anywhere
- Riptide (firmware)
- Rugged Control Center (RCC)
- SD ROM Utility

- SDNAS
- "Server Storage "
- Smart Fabric Storage Software
- SmartByte
- SMI-S
- Software RAID
- Solutions Enabler
- Solutions Enabler vApp
- Sonic
- SRS VE
- Storage Center
- SupportAssist Client Commercial
- SupportAssist Client Consumer
- UCC Edge
- Unisphere for PowerMax
- Unisphere for PowerMax vApp
- Update Manager Plugin
- ViPR Controller
- VNX Control Station
- VNX1
- VNX2
- Vsan Ready Nodes
- Warnado MLK (firmware)
- Wyse Proprietary OS (ThinOS)
- Wyse Windows Embedded Suite

Products Under Review

- Dell Client Platforms (Latitude, OptiPlex, Alienware, Inspiron, Precision, XPS, Vostro, ChengMing) BIOS
- Bare Metal Orchestrator
- Equallogic PS
- ISG Comms
- ISG Drive & Storage Media
- ISG Memory
- Networking SD-WAN Edge VEP Edge

Any security updates or mitigations will be communicated at https://www.dell.com/support/security as soon as they become available. You can subscribe to our Security Alerts to be notified when these Security Advisories are posted by following the guidance here,or by following the directions in the Security Alerts section on the Security Advisories and Notices page.

Recommendations

Customers are encouraged to follow security best practices including those recommended by Apache (Apache Log4j Remote Code Execution) and continue to monitor this notice for further updates as they become available.

Legal Information

Article Properties

Affected Product

Product Security Information

Last Published Date

15 Dec 2021

Version

44

Article Type

Security KB