# Apache Log4j Security Advisory

December 9, 2021, a new critical 0-day vulnerability (CVE-2021-44228) impacting multiple versions of the Apache Log4j 2 logging library was publicly disclosed. ( https://nvd.nist.gov/vuln/detail/CVE-2021-44228)

## Security Advisories / Bulletins linked to Log4Shell (CVE-2021-44228)

https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592

| Vendor | Affected | Not Affected | Security Advisory |
|---|---|---|---|
| **Aruba** | - Silver Peak Orchestrator | - AirWave Management Platform<br>- Aruba Central<br>- Aruba ClearPass Policy Manager<br>- Aruba Instant (IAP)<br>- Aruba NetEdit<br>- Aruba Location Services<br>- Aruba User Experience Insight<br>- ArubaOS Wi-Fi Controllers and Gateways<br>- ArubaOS SD-WAN Controllers and Gateways<br>- ArubaOS-CX switches<br>- ArubaOS-S switches<br>- Aruba VIA Client<br><br>Other Aruba products not listed above are also not known to be affected by<br>the vulnerability. | https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-019.txt |
| **Check Point** | | - Quantum Security Gateway<br>- Quantum Security Management<br>- CloudGuard<br>- Infinity Portal<br>- Harmony Endpoint & Harmony Mobile<br>- SMB<br>- ThreatCloud | https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk176865 |
| **Fortinet** | - FortiAIOps<br>- FortiCASB - **Fixed** on 2021-12-10<br>- FortiConverter Portal - **Fixed** on 2021-12-10<br>- FortiCWP - **Fixed** on 2021-12-10<br>- FortiEDR Cloud - Not exploitable. Additional precautionary mitigations put in place on 2021-12-10 | - FortiADC<br>- FortiAI<br>- FortiAnalyzer<br>- FortiAP<br>- FortiAP-U<br>- FortiAuthenticator<br>- FotiCache<br>- FortiCarrier<br>- FortiClient (All versions)<br>- FortiClientEMS<br>- FortiConnect | https://www.fortiguard.com/psirt/FG-IR-21-245 |

| Vendor | Affected | Not Affected | Security Advisory |
|---|---|---|---|
| | - FortiInsight - Not exploitable. Additional precautionary mitigations being investigated.<br>- FortiIsolator - Fix scheduled for version 2.3.4<br>- FortiMonitor - Not exploitable. Additional precautionary mitigations being investigated.<br>- FortiPortal<br>- FortiPolicy<br>- FortiSIEM<br>ShieldX | - FortiConverter<br>- FortiDDoS<br>- FortiDDoS-F<br>- FortiDeceptor<br>- FortiEDR Agent<br>- FortiExtender<br>- FortiMail<br>- FortiManager<br>- FortiNAC<br>- FortiOS (includes FortiGate & FortiWiFi)<br>- FortiPresence<br>- FortiProxy<br>- FortiRecorder<br>- FortiSandbox<br>- FortiSASE<br>- FortiSOAR<br>- FortiSwitch &<br>- FortiSwitchManager<br>- FortiTester<br>- FortiToken & FortiToken Mobile<br>- FortiVoice<br>- FortiWeb<br>- FortiWLC<br>- FortiWLM<br>- FortiAnalyzer Cloud<br>- FortiClient Cloud<br>- FortiExtender Cloud<br>- FortiGate Cloud<br>- FortiGSLB Cloud<br>- FortiLAN Cloud (includes Switch & AP)<br>- FortiManager Cloud<br>- FortiPenTest<br>- FortiPhish Cloud<br>- FortiToken Cloud<br>- FortiWeb Cloud | |
| **Cisco** | - Cisco Webex Meetings Server<br>- Cisco CX Cloud Agent Software<br>- Cisco Nexus Insights<br>- Cisco Advanced Web Security Reporting Application<br>- Cisco Firepower Threat Defense (FTD) managed by Firepower Device Manager (FDM)<br>- Cisco Identity Services Engine (ISE)<br>- Cisco CloudCenter Cost Optimizer<br>- Cisco CloudCenter Suite Admin<br>- Cisco CloudCenter Workload Manager | - Cisco SocialMiner<br>- Cisco AnyConnect Secure Mobility Client<br>- Cisco Jabber Guest<br>- Cisco Webex App<br>- Cisco Meraki GO Series<br>- Cisco Meraki MR Series<br>- Cisco Meraki MS Series<br>- Cisco Meraki MT Series<br>- Cisco Meraki MV Series<br>- Cisco Meraki MX Series<br>- Cisco Meraki System Manager (SM)<br>- Cisco Meraki Z-Series | https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd |

| Vendor | Affected | Not Affected | Security Advisory |
|---|---|---|---|
|  | - Cisco Crosswork Change Automation<br>- Cisco Crosswork Data Gateway<br>- Cisco DNA Assurance<br>- Cisco Data Center Network Manager (DCNM)<br>- Cisco Evolved Programmable Network Manager<br>- Cisco Intersight Virtual Appliance<br>- Cisco IoT Operations Dashboard<br>- Cisco Network Services Orchestrator (NSO)<br>- Cisco Nexus Dashboard (formerly Cisco Application Services Engine)<br>- Cisco Prime Service Catalog<br>- Cisco WAN Automation Engine (WAE)<br>- Cisco DNA Center<br>- Cisco Network Assurance Engine<br>- Cisco SD-WAN vManage<br>- Unified Computing<br>- Cisco Integrated Management Controller (IMC) Supervisor<br>- Cisco UCS Director<br>- Cisco BroadWorks<br>- Cisco Computer Telephony Integration Object Server (CTIOS)<br>- Cisco Contact Center Domain Manager (CCDM)<br>- Cisco Contact Center Management Portal (CCMP)<br>- Cisco Emergency Responder<br>- Cisco Enterprise Chat and Email<br>- Cisco Finesse<br>- Cisco Packaged Contact Center Enterprise<br>- Cisco Unified Communications Manager / Cisco Unified Communications Manager Session Management Edition<br>- Cisco Unified Communications Manager IM & Presence Service (formerly CUPS)<br>- Cisco Unified Contact Center Enterprise - Live Data server<br>- Cisco Unified Contact Center Enterprise<br>- Cisco Unified Contact Center Express | - Cisco Cloud Services Platform 2100<br>- Cisco Cloud Services Platform 5000 Series<br>- Cisco Extensible Network Controller (XNC)<br>- Cisco Nexus Data Broker<br>- Cisco Tetration Analytics<br>- Cisco Wide Area Application Services (WAAS)<br>- ConfD<br>- Cisco Adaptive Security Appliance (ASA) Software<br>- Cisco Adaptive Security Device Manager<br>- Cisco Content Security Management Appliance (SMA)<br>- Cisco Email Security Appliance (ESA)<br>- Cisco Firepower 4100/9300 Series FXOS Firepower Chassis Manager<br>- Cisco Firepower Management Center<br>- Cisco Security Manager<br>- Cisco Web Security Appliance (WSA)<br>- Cisco ACI Multi-Site Orchestrator<br>- Cisco Application Policy Infrastructure Controller (APIC)<br>- Cisco Business Process Automation<br>- Cisco CloudCenter Action Orchestrator<br>- Cisco Common Services Platform Collector<br>- Cisco Connected Grid Device Manager<br>- Cisco Container Platform<br>- Cisco Elastic Services Controller (ESC)<br>- Cisco IoT Field Network Director (formerly Cisco Connected Grid Network Management System)<br>- Cisco Modeling Labs<br>- Cisco NCS 2000 Shelf Virtualization Orchestrator<br>- Cisco Optical Network Planner<br>- Cisco Policy Suite<br>- Cisco Prime Access Registrar<br>- Cisco Prime Cable Provisioning |  |

| Vendor | Affected | Not Affected | Security Advisory |
|---|---|---|---|
|  | - Cisco Unified Intelligence Center<br>- Cisco Unified Intelligent Contact Management Enterprise<br>- Cisco Unified SIP Proxy Software<br>- Cisco Unity Connection<br>- Cisco Virtualized Voice Browser<br>- Cisco Video Surveillance Operations Manager<br><br>Under Investigation:<br>- Cisco AMP Virtual Private Cloud Appliance<br>- Cisco Secure Network Analytics (SNA) formerly Stealthwatch<br>- Cisco Threat Grid Appliance<br>- Cisco CyberVision Sensor Management Extension<br>- Cisco Virtual Topology System - Virtual Topology Controller (VTC) VM<br>- Cisco Application Policy Infrastructure Controller (APIC) - Enterprise Module<br>- Cisco IOx Fog Director<br>- Cisco Ultra Cloud Core - Access and Mobility Management Function<br>- Cisco Ultra Cloud Core - Session Management Function<br>- Cisco Ultra Cloud Core - Subscriber Microservices Infrastructure<br>- Cisco Paging Server | - Cisco Prime Central for Service Providers<br>- Cisco Prime Collaboration Assurance<br>- Cisco Prime Collaboration Deployment<br>- Cisco Prime Collaboration Provisioning<br>- Cisco Prime IP Express<br>- Cisco Prime Infrastructure<br>- Cisco Prime License Manager<br>- Cisco Prime Network Registrar<br>- Cisco Prime Network<br>- Cisco Prime Optical for Service Providers<br>- Cisco Prime Performance Manager<br>- Cisco Prime Provisioning<br>- Cisco Smart Software Manager On-Prem<br>- Cisco Telemetry Broker<br>- Cisco ACI Virtual Edge<br>- Cisco ASR 5000 Series Routers<br>- Cisco Enterprise NFV Infrastructure Software (NFVIS)<br>- Cisco GGSN Gateway GPRS Support Node<br>- Cisco IOS XR Software<br>- Cisco IOS and IOS XE Software<br>- Cisco IP Services Gateway (IPSG)<br>- Cisco MDS 9000 Series Multilayer Switches<br>- Cisco MME Mobility Management Entity<br>- Cisco Mobility Unified Reporting and Analytics System<br>- Cisco Network Convergence System 2000 Series<br>- Cisco Nexus 3000 Series Switches<br>- Cisco Nexus 5500 Platform Switches<br>- Cisco Nexus 5600 Platform Switches<br>- Cisco Nexus 6000 Series Switches<br>- Cisco Nexus 7000 Series Switches<br>- Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode |  |

| Vendor | Affected | Not Affected | Security Advisory |
|---|---|---|---|
|  |  | - Cisco Nexus 9000 Series Switches in standalone NX-OS mode<br>- Cisco PDSN/HA Packet Data Serving Node and Home Agent<br>- Cisco PGW Packet Data Network Gateway<br>- Cisco SD-WAN vEdge 1000 Series Routers<br>- Cisco SD-WAN vEdge 2000 Series Routers<br>- Cisco SD-WAN vEdge 5000 Series Routers<br>- Cisco SD-WAN vEdge Cloud Router Platform<br>- Cisco System Architecture Evolution Gateway (SAEGW)<br>- Cisco Ultra Packet Core<br>- Cisco HyperFlex System<br>- Cisco UCS C-Series Rack Servers - Integrated Management Controller<br>- Cisco UCS Central Software<br>- Cisco UCS Manager<br>- Cisco Hosted Collaboration Mediation Fulfillment<br>- Cisco Telepresence Endpoints<br>- Cisco Unified Attendant Console Advanced<br>- Cisco Unified Attendant Console Business Edition<br>- Cisco Unified Attendant Console Department Edition<br>- Cisco Unified Attendant Console Enterprise Edition<br>- Cisco Unified Attendant Console Premium Edition<br>- Cisco Unified Communications Domain Manager<br>- Cisco Unified Customer Voice Portal<br>- Cisco Unity Express<br>- Cisco Webex Room Phone<br>- Cisco Expressway Series<br>- Cisco Meeting Server<br>- Cisco TelePresence Management Suite<br>- Cisco TelePresence Video Communication Server (VCS)<br>- Cisco Video Surveillance Media Server |  |

| Vendor | Affected | Not Affected | Security Advisory |
|---|---|---|---|
| | | - Cisco Vision Dynamic Signage Director<br>- Cisco AireOS Wireless LAN Controllers<br>- Cisco Aironet 1560 Series Access Points<br>- Cisco Aironet 1810 Series OfficeExtend Access Points<br>- Cisco Aironet 1810w Series Access Points<br>- Cisco Aironet 1815 Series Access Points<br>- Cisco Aironet 1830 Series Access Points<br>- Cisco Aironet 1850 Series Access Points<br>- Cisco Aironet 2800 Series Access Points<br>- Cisco Aironet 3800 Series Access Points<br>- Cisco Catalyst 9100 Series Access Points<br>- Cisco Catalyst 9800 Series Wireless Controllers<br>- Cisco Connected Mobile Experiences<br>- Cisco Mobility Services Engine | |
| **Palo Alto** | - WildFire Cloud<br>- WildFire Appliance<br>- SaaS Security<br>- Prisma Cloud Compute<br>- Prisma Cloud<br>- Prisma Access<br>- PAN-OS<br>- Okyo Garde<br>- IoT Security<br>- GlobalProtect App<br>- Cortex XSOAR<br>- Cortex Xpanse<br>- Cortex XDR Agent<br>- CloudGenix<br>- Bridgecrew | - | https://security.paloaltonetworks.com/CVE-2021-44228 |
| **Trend Micro** | Under Investigation:<br>- Deep Discovery Director<br>- Trend Micro Web Security<br>- Trend Micro Virtual Patch for Endpoint | - 5G Mobile Network Security<br>- ActiveUpdate<br>- Apex Central (including as a Service)<br>- Apex One (all versions including SaaS, Mac, and Edge Relay)<br>- Cloud App Security<br>- Cloud Edge<br>- Cloud One - Application Security | https://success.trendmicro.com/solution/000289940 |

| Vendor | Affected | Not Affected | Security Advisory |
|---|---|---|---|
|  |  | - Cloud One - Common Services<br>- Cloud One - Conformity<br>- Cloud One - Container Security<br>- Cloud One - File Storage Security<br>- Cloud One - Network Security<br>- Cloud One - Workload Security<br>- Cloud Sandbox<br>- Deep Discovery Analyzer<br>- Deep Discovery Email Inspector<br>- Deep Discovery Inspector<br>- Deep Discovery Web Inspector<br>- Deep Security<br>- Fraudbuster<br>- Home Network Security<br>- Housecall<br>- Instant Messaging Security<br>- Internet Security for Mac (Consumer)<br>- Interscan Messaging Security<br>- Interscan Messaging Security Virtual Appliance (IMSVA)<br>- Interscan Web Security Suite<br>- Interscan Web Security Virtual Appliance (IWSVA)<br>- Mobile Secuirty for Enterprise<br>- Mobile Security for Android<br>- Mobile Security for iOS<br>- MyAccount (Consumer Sign-on)<br>- Network Viruswall<br>- OfficeScan<br>- Password Manager<br>- Phish Insight<br>- Policy Manager<br>- Portable Security<br>- PortalProtect<br>- Public Wifi Protection / VPN Proxy One Pro<br>- Rescue Disk<br>- Rootkit Buster<br>- Safe Lock (TXOne Edition)<br>- Safe Lock 2.0<br>- Sandbox as a Service<br>- ScanMail for Exchange<br>- ScanMail for IBM Domino<br>- Security for NAS<br>- ServerProtect (all versions)<br>- Smart Home Network<br>- Smart Protection Complete<br>- Smart Protection for Endpoints<br>- Smart Protection Server (SPS)<br>- TippingPoint Accessories |  |

| Vendor | Affected | Not Affected | Security Advisory |
|---|---|---|---|
| | | - TippingPoint IPS (N-, NX- and S-series)<br>- TippingPoint Network Protection (AWS & Azure)<br>- TippingPoint SMS<br>- TippingPoint Threat Management Center (TMC)<br>- TippingPoint ThreatDV<br>- TippingPoint TPS<br>- TippingPoint TX-Series<br>- TippingPoint Virtual SMS<br>- TippingPoint Virtual TPS<br>- TMUSB<br>- Trend Micro Email Security & HES<br>- Trend Micro Endpoint Sensor<br>- Trend Micro ID Security<br>- Trend Micro Remote Manager<br>- Trend Micro Security (Consumer)<br>- TXOne (Edge Series)<br>- TXOne (Stellar Series)<br>- Vision One<br>- Worry-Free Business Security (on-prem)<br>- Worry-Free Business Security Services | |
| **SentinelOne** | - 2.15.x is no longer adequate for mitigation purposes | - Version 2.16.0 or newer | https://www.sentinelone.com/blog/cve-2021-44228-staying-secure-apache-log4j-vulnerability/ |
| **F5** | Under Investigation<br>- Traffix SDC (5.x) | - BIG-IP (all modules) 16.x, 15.x, 14.x, 13.x, 12.x, 11.x<br>- BIG-IQ Centralized Management 8.x, 7.x<br>- F5OS 1.x<br>- NGINX Plus R19 - R25<br>- NGINX Open Source 1.x<br>- NGINX Unit 1.x<br>- NGINX App Protect 3.x<br>- NGINX Controller 3.x<br>- NGINX Ingress Controller 2.x, 1.x<br>- NGINX Instance Manager 1.x<br>- NGINX Service Mesh | https://support.f5.com/csp/article/K19026212 |

| Vendor | Affected | Not Affected | Security Advisory |
|---|---|---|---|
| | | 1.x | |
| **Thycotic** | JDBC Proxy Driver | - Secret Server<br>- Privilege Manager<br>- Account Lifecycle Manager<br>- Privileged Behavior Analytics<br>- DevOps Secrets Vault<br>- Connection Manager<br>- Password Reset Server<br>- Cloud Suite<br>- Server Suite | https://docs.thycotic.com/bulletins/current/2021/cve-2021-44228-exploit.md |
| **Elastic** | Elastic Cloud<br>- 7.2 (should restart deployment for the updated setting)<br><br>Logstach<br>- exists on JDKs prior to 8u191<br>- 5.0.0+ up to and including 7.16.0<br><br>APM Java Agent<br>- 1.17.0-1.28.0<br><br>Elasticsearch<br>- 5.x | Elasticsearch<br>- Version 7.16.1, 6.8.21<br>- Version 6.8.9+, 7.8+<br><br>Products:<br>- APM Server<br>- Beats<br>- Cmd<br>- Elastic Agent<br>- Elastic Cloud on Kubernetes<br>- Elastic Endgame<br>- Elastic Maps Service<br>- Endpoint Security<br>- Enterprise Search<br>- Fleet Server<br>- Kibana<br>- Machine Learning | https://discuss.elastic.co/t/apache-log4j2-remote-code-execution-rce-vulnerability-cve-2021-44228-esa-2021-31/291476 |
| **Kiteworks** | No vulnerabilities | No vulnerabilities<br><br>Kiteworks has released the 7.6.1 Hotfix software update | |
| **Nagios** | Under Investigation:<br>Nagios Log Server | Nagios Core, Nagios XI, and Fusion | https://www.nagios.com/news/2021/12/update-on-apache-log4j-vulnerability/ |
| **Order** | No vulnerabilities | Ordr internal IT, Ordr Data Center/AWS | https://resources.ordr.net/blog/ordr-response-to-log4j-vulnerability |
| **Tenable** | | | https://de.tenable.com/sc-dashboards/log4shell-critical-vulnerability?tns_redirect=true |
| **Tripwire** | - Tripwire Industrial Sentinel<br><br>Under Investigation:<br>- Tripwire Connect<br>- Tripwire Connect SaaS<br>- Tripwire Configuration Manager SaaS<br>- Tripwire ExpertOps<br>- Tripwire State Analyzer | - Tripwire® Enterprise<br>- Tripwire IP360™<br>- Tripwire LogCenter®<br>- Tripwire Industrial Visibility<br>- Tripwire Apps<br>- Tripwire Configuration Compliance Manager (CCM)<br>- Tripwire File Analyzer | https://www.tripwire.com/log4j |

| Vendor | Affected | Not Affected | Security Advisory |
|---|---|---|---|
| | | - Tripwire Security Intelligence Hub (SIH)<br>- Tripwire for Servers (TFS) | |