# Allgemein

Update 17.12.2021 - 08:00: Update Citrix, Cisco
Update 16.12.2021 - 08:30: Update Palo Alto Networks
Update 16.12.2021 - 07:45: Update Cisco betroffene Geräte, MobileIron
Update 15.12.2021 - 12:00: Hinzufügen Symantec
Update 15.12.2021 - 07:15: Update Cisco, CISA Referenz hinzugefügt
Update 14.12.2021 - 10:30: Update Citrix, Cisco
Stand 13.12.2021 - 10:00 ist der Großteil der Systeme noch in Untersuchung oder wenn betroffen, sind noch keine Patches verfügbar. Wir versuchen hier einen Überblick zu geben, welche Herstellerprodukte betroffen sind. Für die aktuellsten Infos, bitte direkt die Herstellerseiten besuchen.

Der Fokus liegt **primär** auf Systemen, die von externen/nicht authentifizierten Benutzern von außen erreichbar sind!
Dazu zählen etwa:

- Reverse Proxy
- WLAN Gast Zugänge (Login Portale)
- Sonstige Web Portale, die von extern erreichbar sind

Systeme, die nur von intern erreichbar sind, sind vorerst mal zweitrangig.

Wenn ein Patch oder Workaround verfügbar ist, empfehlen wir diesen schnellstmöglich einzuspielen. Für ein System, für das noch kein Patch veröffentlicht wurde, bleibt nur die Möglichkeit das System herunterzufahren oder den Zugriff massiv einzuschränken.

BSI: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.pdf?__blob=publicationFile&v=3

# Alle Hersteller

BlueTeam CheatSheet * Log4Shell* | Last Updated 2021-12-15 0016 UTC · GitHub
https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592

Übersicht von CISA | 15.12.2021 0400
https://github.com/cisagov/log4j-affected-db

# Diverses

Folgende Dritthersteller werden bei SWS im Collaboration Umfeld eingesetzt:

| | |
|---|---|
| Estos | Nicht betroffen |
| Spectralink | Nicht betroffen |
| Ascom | Nicht betroffen |
| Novalink | Nicht betroffen |
| Recos | Nicht betroffen |
| 2N | Nicht betroffen |
| Peter Connects | Nicht betroffen |

# Cisco

Vulnerability in Apache Log4j Library Affecting Cisco Products | 17.12.2021
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd

**Betroffen**:

| Product | Cisco Bug ID | Fixed Release Availabilty |
|---|---|---|
| Cisco DNA Center | CSCwa47322 | 2.2.2.8 (23 Dec 2021)<br>2.1.2.8 (Jan 2022)<br>2.2.3.4 (Jan 2022) |
| Cisco Identity Services Engine (ISE) | CSCwa47133 | 2.4 hotfix (17 Dec 2021)<br>2.6 hotfix (17 Dec 2021)<br>2.7 hotfix (16 Dec 2021)<br>3.0 hotfix (16 Dec 2021)<br>3.1 hotfix (18 Dec 2021) |
| Cisco UCS Director | CSCwa47288 | 6.8.2.0 (22 Dec 2021) |
| Cisco Firepower Threat Defense (FTD) managed by Firepower Device Manager (FDM) | CSCwa46963 | 6.2.3 hotfix (23 Dec 2021)<br>6.4.0 hotfix (23 Dec 2021)<br>6.6.5 hotfix (23 Dec 2021)<br>7.0.1 hotfix (23 Dec 2021)<br>7.1.0 hotfix (23 Dec 2021) |

***NICHT* betroffen:**

- Cisco AnyConnect Secure Mobility Client
- Cisco ASA
- Cisco Content Security Management Appliance (SMA)
- Cisco Email Security Appliance (ESA)
- Cisco Expressway Series
- Cisco Firepower Management Center
- Firepower Thread Defense (FTD) managed by Cisco Firepower Management Center
- Cisco IOS
- Cisco IOS XE
- Cisco IOS XR
- Cisco Jabber Guest
- Cisco Nexus 3000/5500/5600/6000/7000/9000 Switches
- Cisco Meraki (MR, MS, MT, MV, MX, SM, Z)
- Cisco UCS Manager
- Cisco Webex App
- Cisco Web Security Appliance (WSA)

# Citrix

Citrix Security Advisory for Apache CVE-2021-44228 | 17.12.2021

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

| Product | Status |
|---|---|
| Citrix ADC (NetScaler ADC) and Citrix Gateway (NetScaler Gateway) | Not impacted (all platforms) |
| Citrix Application Delivery Management (NetScaler MAS) | Not impacted (all platforms) |
| Citrix Cloud Connector | Not impacted |
| Citrix Connector Appliance for Cloud Services | Not impacted |
| Citrix Endpoint Management (Citrix XenMobile Server) | Impacted – Customers are advised to apply the latest CEM rolling patch updates listed below as soon as possible to reduce the risk of exploitation<br>• XenMobile Server 10.14 RP2: https://support.citrix.com/article/CTX335763<br>• XenMobile Server 10.13 RP5: https://support.citrix.com/article/CTX335753<br>• XenMobile Server 10.12 RP10: https://support.citrix.com/article/CTX335785 |
| Citrix Hypervisor (XenServer) | Not impacted |
| Citrix License Server | Not impacted |

| | |
|---|---|
| Citrix SD-WAN | Not impacted (all platforms) |
| Citrix ShareFile Storage Zones Controller | Not impacted |
| Citrix Virtual Apps and Desktops (XenApp & XenDesktop) | Impacted – Linux VDA (non-LTSR versions only)<br><br>Customers are advised to apply the latest update as soon as possible to reduce the risk of exploitation<br><br>• Linux Virtual Delivery Agent 2112: https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/linux-vda-2112.html<br><br>Mitigations:<br><br>Customers who are not able to upgrade immediately can execute the following commands with root privileges on the Linux machine running VDA:<br><br>cd /opt/Citrix/VDA/lib64<br><br>zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class<br><br>Not Impacted – Linux VDA LTSR all versions<br><br>Not Impacted – All other CVAD components |
| Citrix Workspace App | Not impacted (all platforms) |

Citrix empfiehlt ADC Kunden den Einsatz von Responder Policies (s. Link oben)

# MobileIron

https://forums.ivanti.com/s/article/Security-Bulletin-CVE-2021-44228-Remote-code-injection-in-Log4j?language=en_US
Workaround verfügbar (Installation eines RPM Moduls)
Betroffen:

- MobileIron Core
- MobileIron Sentry
- Core Connector
- Reporting Database (RDB)

*Nicht* betroffen:

- MobileIron Cloud

# NetApp

https://security.netapp.com/advisory/ntap-20211210-0007/

| **Product** | **Status** | **Workaround** | **Patch** |
|---|---|---|---|
| SnapCenter Plug-in for VMware vSphere | affected | CVE-2021-44228 Apache Log4j Vulnerability in NetApp Products \| NetApp Product Security -> Remediation | Nicht verfügbar (13.12.) |

# PaloAltoNetworks

https://security.paloaltonetworks.com/CVE-2021-44228

**Betroffen:**

| | |
|---|---|
| PAN-OS for Panorama | 9.0.*, 9.1.*, 10.0.* |

***Nicht* betroffen:**

- PAN-OS for Firewall and Wildfire
- .. alle weiteren Palo Alto Networks Produkte sind nicht betroffen.

# RedHat

https://access.redhat.com/security/vulnerabilities/RHSB-2021-009

Workaround für Container die nicht gepatcht werden können ENV LOG4J_FORMAT_MSG_NO_LOOKUPS=true

# Sophos

Advisory: Log4j zero-day vulnerability AKA Log4Shell (CVE-2021-44228) | Sophos

| Product | Status | Patch |
|---|---|---|
| Sophos Central | Not impacted | |
| Sophos Firewall (all versions) | Not vulnerable | |
| SG UTM (all versions) | Not vulnerable | |
| SG UTM Manager (SUM) (all versions) | Not vulnerable | |
| Sophos Mobile EAS Proxy | ***Impacted*** | download and install version 9.7.2, available from Monday December 13, 2021, on the same machine where it is currently running. |
| Sophos Mobile | Not impacted | |

# Symantec (Broadcom)

https://support.broadcom.com/security-advisory/content/security-advisories/Symantec-Security-Advisory-for-Log4j-2-CVE-2021-44228-Vulnerability/SYMSA19793

# Veeam

https://www.veeam.com/kb4254

Nichts betroffen. Log4j wird in keinem Veeam Produkt genutzt

# VMware

VMSA-2021-0028.2 (vmware.com)

| Product | Status | Workaround |
|---|---|---|
| VMware vCenter Server Appliance | V7.x, 6.7.x, 6.5.x affected | https://kb.vmware.com/s/article/87081?lang=en_US |
| VMware vCenter Server Windows | V6.7.x, 6.5.x affected | https://kb.vmware.com/s/article/87096 |
| VMware Site Recovery Manager, vSphere Replication | V8.3, 8.4, 8.5 affected | https://kb.vmware.com/s/article/87098 |
| VMware vCenter Cloud Gateway | V1.x affected | https://kb.vmware.com/s/article/87081 |
| VMware vRealize Log Insight | V8.2, 8.3, 8.4, 8.6 affected | https://kb.vmware.com/s/article/87089 |