# WICHTIGE SECURITY INFORMATION: Logj4 Schwachstelle

In der weit verbreiteten Java-Bibliothek Log4j wurde eine Zero-Day-Schwachstelle (CVE-2021-44228) entdeckt, die in der CVSSv3 Skala mit 10 Punkten die höchste Bewertung erhalten hat. Dementsprechend kritisch ist diese Schwachstelle, da Angreifer darüber beliebigen Code ausführen lassen können. Über manipulierte Anfragen an einen verwundbaren Server oder eine betroffene Anwendung ist dadurch sogar eine vollständige Übernahme des betroffenen Systems möglich.

Viele Hersteller aus unserem Portfolio bieten bereits Updates an, um diese Schwachstelle zu schließen oder einzuschränken. Für Log4j unter Apache gibt es bereits einen Hotfix, aber für andere Anwendungen, die log4j enthalten, fehlen leider noch Updates. Die Angaben zu den Updates sind derzeit noch nicht vollständig überschaubar und daher im Einzelfall zu prüfen. Wir erwarten, dass in den nächsten Tagen weitere Produkte als verwundbar erkannt werden.

**Es folgt eine Übersicht der Hersteller, und der jeweilige Status soweit uns dieser derzeit bekannt ist. Bitte prüfen Sie in den nächsten Tagen aktiv, ob die Hersteller unter den angeführten Links Updates veröffentlichen.**

| Hersteller | Status | Version | Link zur Knowledge Base |
|---|---|---|---|
| Check Point | Nicht verwundbar | | Siehe KB |
| Cyber Ark | Ja | - Privilege Threat Analytics (alle Versionen<br>-Remote Access Connector (Version 1.0.12409 und davor) | Siehe KB |
| Trend Micro | in Prüfung | | Siehe KB |
| RSA | Ja | -SecurID Authentication Manager 8.6 Patch 1 | Siehe KB |
| Radware | teilweise verwundbar oder noch in Prüfung | -KWAF<br>-BotManager Connectors<br>-Defense Flow (Version 4.2.x und davor)<br>-Vision (Versionen vor 4.83)<br>-vDirect | Siehe KB |
| VMWare | in Prüfung | | Siehe KB |
| Thales | in Prüfung | | Siehe KB |
| Netapp | in Prüfung | | Siehe KB |
| Cisco | in Prüfung | | Siehe KB |
| Nutanix | teilweise verwundbar oder noch in Prüfung | | Siehe KB |
| Commvault | teilweise verwundbar | Einige Agents könnten betroffen sein | Siehe KB |
| Veritas Netbackup | ja | -NetBackup Primary Server 8.1 - 8.1.1 | Siehe KB |

| | | | |
|---|---|---|---|
| | | -NetBackup Primary Server 8.1.2 - 9.1.0.1<br>-NetBackup CloudPoint 8.3 - 9.1.0.1<br>-NetBackup Primary Server container auf Flex Appliance 8.1.2 - 9.1.0.1 mit Flex<br>-NetBackup Resiliency Platform 3.6 - 4.0 | |
| Splunk | teilweise verwundbar oder noch in Prüfung | | Siehe KB |

Einige unserer Partner und Hersteller bieten Möglichkeiten zur Erkennung oder sogar zur Abwehr von Angriffen an, die diese Schwachstelle betreffen:

- Check Point bietet eine IPS Signatur an, um verwundbare Systeme zu schützen
- Trend Micro bietet ebenfalls Möglichkeiten zur Erkennung und zum Schutz vor Angriffen zu dieser Schwachstelle
- Splunk ermöglicht es potenziell infizierte Systeme zu erkennen. siehe KB
- Radware schützt durch Web-Application Security Lösungen mit entsprechenden Signaturen. siehe KB
- Rapid7 und Tenable haben ebenfalls Signaturen zur Erkennung in ihren Vulnerability Scanning Lösungen bereitgestellt
- Die Endpoint Detection Response (EDR) Systeme von Check Point, Trend Micro und Rapid7 ermöglichen über die Threat Hunting Funktion eine gezielte Suche nach verwundbaren Systemen

**Infoquellen/Referenzen:**

https://logging.apache.org/log4j/2.x/security.html

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

https://github.com/YfryTchsGD/Log4jAttackSurface

**Unsere empfohlenen Maßnahmen dazu:**

Folgen Sie den Hinweisen der Hersteller und führen Sie die entsprechenden Update Schritte durch. Derzeit sind uns keine weiteren Details anderer Hersteller und Lösungen bekannt. Wir werden diese gegebenenfalls in einem Update nachliefern.

Bei Fragen zu diesem Thema unterstützen wir Sie gerne unter **support@bacher.at** oder +43 60 126-34. Falls die erforderliche Maßnahme nicht durch Ihren Betriebsführungs- oder Support-Vertrag abgedeckt ist, bieten wir Ihnen auf Rückfrage gerne an, die Arbeiten durch unsere Spezialisten durchzuführen.

## English version

The widely used Java-Library Log4j is affected by a zero-day vulnerability (CVE-2021-44228) with the highest CVSSv3 Score 10. This critical issue could potentially be exploited by a remote attacker to execute arbitrary code. Manipulated requests to a vulnerable server or application may lead to a full takeover of the system.

Several of our vendors already delivered updates to patch this vulnerability or to mitigate it. Keep in mind that Log4j used on Apache webserver can be patched already but applications using Log4j may still have no update. Be aware that the full impact and available updates are not completely explored and may change within the next days.

**Here is a list of vendors and their status on vulnerability and software updates. Please monitor the given links for possible changes actively over the next days.**

| Vendor | Status | Version | Link to knowledge base |
|---|---|---|---|
| Check Point | not vulnerable | | See KB |
| Cyber Ark | yes | - Privilege Threat Analytics (alle Versionen<br>-Remote Access Connector (Version 1.0.12409 und davor) | See KB |
| Trend Micro | under investigation | | See KB |
| RSA | Yes | -SecurID Authentication Manager 8.6 Patch 1 | See KB |
| Radware | partially vulnerable or under investigation | -KWAF<br>-BotManager Connectors<br>-Defense Flow (version 4.2.x und davor)<br>-Vision (versions priot to 4.83)<br>-vDirect | See KB |
| VMWare | under investigation | | See KB |
| Thales | under investigation | | See KB |
| Netapp | under investigation | | See KB |
| Cisco | under investigation | | See KB |
| Nutanix | partially vulnerable or under investigation | | See KB |
| Commvault | partially vulnerable | some agents may be affected | See KB |

| | | | |
|---|---|---|---|
| Veritas Netbackup | yes | -NetBackup Primary Server 8.1 - 8.1.1<br>-NetBackup Primary Server 8.1.2 - 9.1.0.1<br>-NetBackup CloudPoint 8.3 - 9.1.0.1<br>-NetBackup Primary Server container on Flex Appliance 8.1.2 - 9.1.0.1 running on Flex<br>-NetBackup Resiliency Platform 3.6 - 4.0 | See KB |
| Splunk | partially vulnerable | | See KB |

Some of our partners and vendors provide detection or even prevention methods related to this kind of attacks:

- Check Point released IPS signatures to protect vulnerable systems
- Trend Micro too released possible mitigations for this vulnerability
- Splunk allows detection of infected hosts See KB
- Radware protects using web application security solutions with relevant signatures See KB
- Rapid7 and Tenable also released signatures for their vulnerability scanning solutions
- Endpoint Detection Response (EDR) systems from Check Point, Trend Micro und Rapid7 allow targeted search for vulnerable systems using threat hunting functions

**Sources/references:**

https://logging.apache.org/log4j/2.x/security.html

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

https://github.com/YfryTchsGD/Log4jAttackSurface

**Our recommendation:**

Follow the given procedures for each solution and implement the updates. Any possible updates on our part will be communicated by additional information.

We are at your disposal in case you need assistance or if you have questions. You can contact us at **support@bacher.at** or +43 1 60 126-34. In case this is not already covered by your operational contract we gladly offer on request to have this change implemented by one of our engineers.