

Schwachstellen beheben: Gezielter, schneller und einfacher arbeiten

mit Autobahn Security

Alexis Tenzler
Head of Customer Success

it-sa Expo 2022

Zitate von IT-Security Experten und CISOs



„Meine IT-Administratoren wehren sich, weil sie die Relevanz nicht kennen.“



„Mein Team ist ausgelastet!“



„Ich interessiere mich nicht für eine hohe Anzahl an Funden, sondern speziell für die Schwachstellen, die tatsächlich ausgenutzt werden können.“

Was leisten Schwachstellenscanner?

Und was nicht?



Finden von IT-Assets
(Asset discovery)



Finden von
Schwachstellen in der
Infrastruktur



Priorisierung der
Schwachstellen



...Schwachstellen gruppieren



...Beseitigung der Ursachen von
Schwachstellen



...Anleitung zur Behebung bereitstellen



...Messen das Niveau Ihrer IT-
Sicherheit

Autobahn Security skaliert Expertenwissen

Wir machen aus Tausenden Problemen eine Handvoll priorisierter Aufgaben

Integrieren aller Schwachstellen



25 umsetzbare Cyber-Fitness-Workouts

Falsch Positive und irrelevante Schwachstellen eliminieren

Dubletten entfernen und Schwachstellen gruppieren

Den Schwachstellengruppen die Lösungsanweisung zuweisen

Weniger und gezielter arbeiten durch Gruppierung

Cyber Fitness Workouts sind konzipiert um maximale Wirkung erzielen und Ihnen wertvolle Zeit sparen

The image shows a screenshot of the Cyber Fitness interface. On the left is a sidebar with navigation links: Dashboard, Workouts, Scanning, Assets, Issues (highlighted), Team, and Integrations. The main area displays a table of issues with columns for Issue and Severity. Several issues are highlighted with red boxes, and a red circle with a dumbbell icon is placed over the table, with arrows pointing to a detailed view on the right.

Issue	Severity
Oracle 11.2.0.3.0 on Micr...	Medium
Oracle Enterprise Linux R...	Low
Oracle Enterprise Linux S...	Critical
Oracle Enterprise Linux S...	High
Oracle Enterprise Linux S...	Medium
Oracle Enterprise Linux S...	Medium
Oracle Enterprise Linux S...	Medium
Oracle Enterprise Linux S...	High
Oracle Enterprise Linux S...	Medium
Oracle Enterprise Linux S...	Medium

Navigation: < 1 ... 9 10 11 12 13 ... 18 > 10 / page

Patch your Oracle Linux

Open PDF Mark workout as ▾

Warm up Setup Workout

EFFORT ⓘ	HACKABILITY SHARE	HOST(S)
Small	14.55% Since 13 Oct 2022 00:00	13

Description

Oracle Linux is a Linux distribution packaged and freely distributed by Oracle, available partially under the GNU General Public License since late 2006. It is compiled from Red Hat Enterprise Linux source code.

Risk

An adversary might use publicly available exploits to gain access to your system as there are various software packages installed on your server that are missing updates. Depending on the specific

Schneller mehr Verbesserung erzielen durch Priorisierung

Aus dem Hackability Share lesen Ihre IT-Administratoren das Verbesserungspotential ab

The image displays two screenshots from the 'Cyber Fitness' application. The left screenshot shows a detailed view of a workout titled 'Patch your Oracle Linux'. The right screenshot shows a list of various workouts.

Left Screenshot: Patch your Oracle Linux

Buttons: Open PDF, Mark workout as ▾

Tabs: Warm up (selected), Setup, Workout

EFFORT 📊
Small

HACKABILITY SHARE
14.55%
Since 13 Oct 2022 00:00

HOST(S)
13

Description
Oracle Linux is a Linux distribution packaged and freely distributed by Oracle, available partially under the GNU General Public License since late 2006. It is compiled from Red Hat Enterprise Linux source code.

Risk
An adversary might use publicly available exploits to gain access to your system as there are various software packages installed on your server that are missing updates. Depending on the specific

Right Screenshot: Cyber Fitness Workouts

Workout	Assignee	Hackability share	Effort	Status	Action
Patch your Red Hat Enterprise Linux	AV Arjen Vogel	27.26 %	Small	To do	⋮
Patch your Oracle Linux	AP Ade Pratama	14.55 %	Small	To do	⋮
Patch NGINX servers	AM Ana Maria	13.24 %	Medium	To do	⋮
Patch Microsoft Office	AM Ana Maria	13.24 %	Small	To do	⋮
Patch Ubuntu Linux	JP Julia Pardo	12.98 %	Small	To do	⋮
Patch Oracle databases	JP Julia Pardo	12.98 %	Medium	To do	⋮

Cyber Fitness Workouts - Gezielter, schneller und einfacher

Warm up

Back to workouts

Patch Apache Log4j

Open PDF Mark workout as

Warm up Setup Workout

EFFORT

Medium

HACKABILITY SHARE

57.90%

Since 24 Oct 2022 00:00

HOST(S)

26

Description

Log4j service by Apache is one of the most common tools for sending text to be stored in log files and/or databases. It is used in a lot of applications and websites to log messages according to message type and level. For example, it can keep track of website visitors or note when warnings or errors occur in processing.

Risk

Log4j not only logs strings; text strings that are formatted in a certain way will be executed just like a line from a computer program. The problem here is that an adversary might get the ability to manipulate computers by running malicious strings without the computer owners' permission. For example, the `${jndi:ldap}` path allows arbitrary code to be loaded from a remote URL. Apart from the dangers of the remote code execution, denials of service are also possible.

Objective

In this workout, we patch Apache Log4j to fix the remote code execution vulnerability called Log4Shell. As a critical flaw, it needs to be addressed immediately.

- Follow the below men...
- Remediation option 1 - Upgrade the vulnerable versions
- Remediation option 2 - Setting system properties
- Remediation option 3 - pom.xml fix
- Remediation option 4 - Azure App Service (Windows and Linux)
- Remediation option 5 - Any containerized applications

Cyber Fitness Workouts - Gezielter, schneller und einfacher

Remediation Step 2

Back to workouts

Patch Apache Log4j

Open PDF Mark workout as

Warm up Setup **Workout**

- Remediation step 1
Follow the below men...
- Remediation step 2**
Remediation option 1 - Upgrade the vulnerable versions
- Remediation step 3
Remediation option 2 - Setting system properties
- Remediation step 4
Remediation option 3 - pom.xml fix
- Remediation step 5
Remediation option 4 - Azure App Service (Windows and Linux)
- Remediation step 6
Remediation option 5 - Any containerized applications

Patch Apache Log4j

2/6

Remediation option 1 - Upgrade the vulnerable versions

The good news is that not all versions of Log4j are equally affected by the Log4Shell issue. The affected 2.x **Log4Shell versions are as follows: all log4j-core versions ≥ 2.0 -beta9 and $\leq 2.14.1$. Their users should consider the following migration paths:

- For Java 8 (or later), users should upgrade to release 2.17.x
- For Java 7, users should upgrade to 2.12.2. This upgrade contains a security patch for this vulnerability

Note

Only log4j-core JAR file is impacted by this vulnerability. Applications using only the log4j-api JAR file without the log4j-core file are not affected by this vulnerability. Log4j 1.x does not have lookups, so the risk is lower. Likewise, configurations without JMSAppender are not affected

To upgrade Log4j, take the three steps outlined below.

- ☐ **1 - Download Log4j**
 - Download the latest version of Log4j from the [download page](#)
 - Unzip the file in a local directory — for example, C:\Workspace\example.com\lib\apache-log4j-core-[version]-bin
- ☐ **2 - (for Windows) Add Log4j to the System Environment variable path and ClassPath**
 - Navigate to the **Search** menu and type **About your PC**
 - From the window that appears, click **Advanced system settings** → **Environment Variables** → **Path**
 - Add your log4j directory path to the value: C:\Workspace\example.com\lib\apache-log4j-core-[version]-bin
 - Add log4j-api.jar to the **ClassPath** system environment variable by following the above steps
- ☐ **2 - (for Linux) Add Log4j to the System Environment variable path and ClassPath**

In Linux terminal, run the following command:

```
export CLASSPATH=$CLASSPATH:/usr/local/apache-log4j-core-[version]-bin/log4j-[version].jar
export PATH=$PATH:/usr/local/apache-log4j-[version]-bin/
```

Cyber Fitness Workouts - Gezielter, schneller und einfacher

Remediation Step 4

← Back to workouts

Patch Apache Log4j

Open PDF Mark workout as ✓

Warm up Setup **Workout**

- Remediation step 1
Follow the below men...
- Remediation step 2
Remediation option 1 - Upgrade the vulnerable versions
- Remediation step 3
Remediation option 2 - Setting system properties
- **Remediation step 4**
Remediation option 3 - pom.xml fix
- Remediation step 5
Remediation option 4 - Azure App Service (Windows and Linux)
- Remediation step 6
Remediation option 5 - Any containerized applications

Patch Apache Log4j 4/6

Remediation option 3 - pom.xml fix

Update the dependency in the pom.xml file with the latest available version:

```
<dependency>  
  <groupId>org.apache.logging.log4j</groupId>  
  <artifactId>log4j</artifactId>  
  <version>2.15.0</version>  
  <type>pom</type>  
</dependency>
```

You can find the latest available version at: <https://search.maven.org/artifact/org.apache.logging.log4j/log4j/2.15.0/pom>

← Previous Next →

Cyber Fitness Workouts - Gezielter, schneller und einfacher

Remediation Step 5

Back to workouts

Patch Apache Log4j

Open PDF Mark workout as

Warm up Setup Workout

- Remediation step 1
Follow the below men...
- Remediation step 2
Remediation option 1 - Upgrade the vulnerable versions
- Remediation step 3
Remediation option 2 - Setting system properties
- Remediation step 4
Remediation option 3 - pom.xml fix
- Remediation step 5**
Remediation option 4 - Azure App Service (Windows and Linux)
- Remediation step 6
Remediation option 5 - Any containerized applications

Patch Apache Log4j 5/6

Remediation option 4 - Azure App Service (Windows and Linux)

It is recommended to upgrade Log4j to version v2.17.x and redeploy your applications.

If you are not able to redeploy your application, then in log4j ≥ 2.10 you can mitigate this behavior by setting the system property `Dlog4j2.formatMsgNoLookups=true`.

On App Service, you can set this property by creating an app setting named `JAVA_OPTS` with the following configuration settings:

```
az webapp config appsettings set --name <app-name> --resource-group <resource-group-name> --settings JAVA_OPTS="--Dlog4j2.formatMsgNoLookups=true"
```

Previous Next

Zitate von IT-Security Experten und CISOs



„Meine IT-Administratoren wehren sich, weil sie die Relevanz nicht kennen.“



„Mein Team ist ausgelastet!“



„Ich interessiere mich nicht für eine hohe Anzahl an Funden, sondern speziell für die Schwachstellen, die tatsächlich ausgenutzt werden können.“

Zitate von IT-Security Experten und CISOs



„Meine IT-Administratoren kennen die Relevanz jedes Tickets, bzw. jeder Anleitung.“



„Ich weiß, welche Arbeiten ich zuerst angehen will.“



„Mein Team hat weiterhin viel zu tun, treibt aber jetzt die digitale Roadmap voran.“

Besuchen Sie uns
für eine Live-Demo
Stand 7-242 in Halle 7