

# Utimaco Security Bulletin

Utimaco Products Affected by Log4J Vulnerabilities

(CVE-2021-44228, CVE-2021-44832, CVE-2021-45046, CVE-2021-45105)



## Imprint

Copyright 2021      Utimaco GmbH  
Germanusstr. 4  
D-52080 Aachen  
Germany

Phone                AMERICAS +1-844-UTIMACO (+1 844-884-6226)  
EMEA +49 800-627-3081  
APAC +81 800-919-130

Author

Creation Date      16 Dec 2021

Rev.                 2.0

Rev. Date          18 Jan 2022

Status

Export Date        27 Jan 2022

Internet             [www.utimaco.com](http://www.utimaco.com)  
e-mail               [quality-management@utimaco.com](mailto:quality-management@utimaco.com)

All rights reserved

No part of this documentation may be reproduced in any form (printing, photocopy or according to any other process) without the written approval of Utimaco GmbH or be processed, reproduced or distributed using electronic systems.

Utimaco GmbH reserves the right to modify or amend the documentation at any time without prior notice. Utimaco GmbH assumes no liability for typographical errors and damages incurred due to them.

All trademarks and registered trademarks are the property of their respective owners.

# Table of Contents

- 1 Who should read this bulletin? ..... 4**
- 1.1 Overview - Impacted Products..... 4
- 2 Summary ..... 4**
- 3 Change History ..... 5**
- 4 Impact of Vulnerability and Mitigation Steps..... 6**
- 4.1 Utimaco Products - Impacted..... 6
- 4.2 Mitigation Factors ..... 7
- 4.3 Support..... 7
- 4.3.1 EMEA ..... 7
- 4.3.2 AMERICAS ..... 7
- 4.3.3 APAC ..... 7

## 1 Who should read this bulletin?

Utimaco has triaged products for impact from CVE-2021-44228, CVE-2021-44832, CVE-2021-45046 and CVE-2021-45105. Products that have been investigated and have reached a conclusion of "Impacted" are listed in this bulletin, along with mitigation steps.

Any products not listed in this bulletin are evaluated as "Not Affected" at the time of publication. If you have questions, please contact Utimaco Support for the most up to date information

### 1.1 Overview - Impacted Products

The following products have been found to be **Impacted** by

- CVE-2021-44228
- CVE-2021-44832
- CVE-2021-45046
- CVE-2021-45105

Details on each product can be found below.

- ESKM v8
- u.trust Identify

## 2 Summary

On December 10, 2021, details emerged about a critical remote code execution vulnerability in Apache Log4j, assigned as CVE-2021-44228, in which users who can cause specifically crafted strings to be processed by an application's Log4j logging layer may be able to execute code and thereby take control of the server hosting the affected application. On December 14, 2021, a second vulnerability in Apache Log4j, CVE-2021-45046, was identified. This second vulnerability identifies that, despite the changes made in Log4j 2.15.0 (and the similar effect of applying an environment variable-based or system property-based mitigation), there could remain cases where arbitrary code execution could be achieved. Two more log4j vulnerability have been identified in the following days: CVE-2021-44832 and CVE-2021-45105.

The official security advisory from Apache describing these issues can be found here:

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

Utimaco has investigated the impact of all listed vulnerabilities on all products. Utimaco is continuing to monitor and assess ongoing product impacts and will take additional action as necessary. In the interest of releasing this bulletin in a timely manner, investigations into the

details of product impacts, as well as patch availability timelines, are still ongoing. As such, information below should be considered preliminary. Utimaco will release more communications, as needed, as these investigations proceed.

### 3 Change History

<i>Rev. No.</i>	<i>Date Published</i>	<i>Major Changes</i>
1.0		Initial version
2.0		Updated version, adding two more log4j vulnerabilities

## 4 Impact of Vulnerability and Mitigation Steps

Products that have been investigated and have reached a conclusion of "Impacted" at time of publication are listed below. Please note that some products are still under investigation. For any products not listed in this bulletin contact Utimaco Support for the most up to date information.

### 4.1 Utimaco Products - Impacted

This table includes Utimaco products that have exposure to the listed CVEs. As per the Apache Log4j security advisory, Utimaco is expediting patches for all affected products that update Log4j to version 2.17.1 or later.

<b>Product</b>	<b>Version(s)</b>	<b>Impact</b>	<b>Corrective Actions</b>
u.trust Identify	<ul style="list-style-type: none"> <li>▪ Release 1.2.0, 1.3.0               <ul style="list-style-type: none"> <li>• Please note that <i>u.trust Identify</i> was formerly known as <i>except Connect Identify</i></li> <li>• All components except for CMS-Web</li> </ul> </li> </ul>	Remote Code Execution	<ul style="list-style-type: none"> <li>▪ Limit access to vulnerable systems</li> <li>▪ Apply 1.4.2 update               <ul style="list-style-type: none"> <li>• u.trust Identify 1.4.2 is available on the former except Download Platform</li> </ul> </li> </ul>
ESKM	v8.x	Remote Code Execution	<ul style="list-style-type: none"> <li>▪ Limit access to vulnerable systems</li> <li>▪ Apply 8.4 update               <ul style="list-style-type: none"> <li>• ESKM v8.4 updates the Log4j to v2.17.1 to fix the reported vulnerabilities.</li> </ul> </li> </ul>

## 4.2 Mitigation Factors

Exploitation of CVE-2021-44228 requires that an attacker cause the server running Log4j to open a network connection to a remote host running a malicious application. It is possible to protect application servers running vulnerable Log4j implementations by implementing network controls that prevent that server from opening connections to untrusted networks or hosts. An example of such a policy would be to use onboard firewall software, or network zone firewalls to prevent servers from opening connections to the internet. Please work with your network and technology teams as blocking outgoing connections may affect legitimate functionality of a server or application.

## 4.3 Support

### 4.3.1 EMEA

<b>E-Mail:</b>	support@utimaco.com
<b>Tel.:</b>	+49 241 16 96 155

### 4.3.2 AMERICAS

<b>E-Mail:</b>	support@utimaco.com
<b>Tel.:</b>	+1-844-UTIMACO

### 4.3.3 APAC

<b>E-Mail:</b>	support@utimaco.com
<b>Tel.:</b>	+81 800-919-1301