Utimaco Security Bulletin

Utimaco Products Affected by Log4J Vulnerabilities (CVE-2021-44228, CVE-2021-45046)

utimaco®

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.	1.0
Rev. Date	16 Dec 2021
Status	
Export Date	17 Dec 2021

Internet	www.utimaco.com
e-mail	quality-management@utimaco.com

Table of Contents

1 Who should read this bulletin? 4

1.1 Overview - Impacted Products 4

2 Summary 4

3 Change History 4

4 Impact of Vulnerability and Mitigation Steps 5

4.1 Utimaco Products - Impacted 5

4.2 Mitigation Factors 6

4.3 Support 6

4.3.1 EMEA 6

4.3.2 AMERICAS 6

4.3.3 APAC 6

1 Who should read this bulletin?

Utimaco has triaged products for impact from CVE-2021-44228 and CVE-2021-45046. 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 and CVE-2021-45046. 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.

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 CVE-2021-44228 and CVE-2021-45046 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

Rev. No.	***Date Published***	***Major Changes***
1.0		Initial version

Rev. No.	*Date Published*	*Major Changes*

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 CVE-2021-44228. As per the Apache Log4j security advisory, Utimaco is expediting patches for all affected products that update Log4j to version 2.16.0 or later.

Product	*Version(s)*	*Impact*	*Corrective Actions*
u.trust Identify	▪ Release 1.2.0, 1.3.0 • Please note that *u.trust Identify* was formerly known as *exceet Connect Identify* • All components except for CMS-Web	Remote Code Execution	▪ Limit access to vulnerable systems ▪ Apply hot fix • Immediate hot fix 1.2.1 is available on the former exceet Download Platform • 1.3.1 work in progress
ESKM	v8.x	Remote Code Execution	▪ Limit access to vulnerable systems ▪ Apply hot fix • Immediate hot fix is available with Utimaco Support • v8.3.2 that patches the

Product	*Version(s)*	*Impact*	*Corrective Actions*
			vulnerability is in progress

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

E-Mail:	support-cs@utimaco.com support-atalla@utimaco.com
Tel.:	+49 241 16 96 155

4.3.2 AMERICAS

E-Mail:	support-cs@utimaco.com support-atalla@utimaco.com
Tel.:	+1-844-UTIMACO

4.3.3 APAC

E-Mail:	support-cs@utimaco.com support-atalla@utimaco.com
Tel.:	+49 241 16 96 155