

# 了解Cisco Contact Center解决方案中Apache Log4j漏洞的影响

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[ICM服务器上的Tomcat版本检查](#)

[常见问题](#)

## 简介

本文档介绍Apache Log4j漏洞对Cisco Contact Center(UCCE)产品线的影响。

## 先决条件

### 要求

本文档没有任何特定的要求。

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Unified Contact Center产品版本11.6及更高版本。

## 背景信息

Apache最近宣布Log4j组件中存在漏洞。它广泛用于思科联系中心解决方案，思科积极评估产品组合，以验证哪些产品是安全的，哪些产品受到影响。

**注意：** 有关详细信息，请[访问：思科安全建议 — cisco-sa-apache-log4j](#)

本文档在可用时提供更多信息。

	<b>ID</b>	<b>11.6.(2)</b>	<b>12.0(1)</b>	<b>12.5(1)</b>	<b>12.6(1)</b>
UCCE/ICM	<a href="#">CSCwa47273</a>	<a href="#">补丁 — 11.6(2) ES84 自述</a>	<a href="#">补丁 — 12.0(1) ES91 自述</a>	<a href="#">补丁 — 12.5(1) ES101 自述</a> 注释 1：需要ES_55修补程序，请参阅 <a href="#">OpenJDK迁移文档</a> 注释 2：Tomcat版本检查 —	<a href="#">补丁 — 12.6(1) ES 自述</a>

请参阅下面的“ICM服务器上的Tomcat版本检查”部分

PCCE	<a href="#">CSCwa47274</a>	<a href="#">补丁 — 11.6(2) ES84 自述</a>	<a href="#">补丁 — 12.0(1) ES91 自述</a>	<a href="#">补丁 — 12.5(1) ES101 自述</a> 注释 1：需要ES_55修补程序，请参阅 <a href="#">OpenJDK迁移文档</a> 。 注释 2：Tomcat版本检查 — 请参阅下面的“ICM服务器上的Tomcat版本检查”部分	<a href="#">补丁 — 12.6(1) ES101 自述</a>
CTIOS		不受影响	不受影响	不受影响	不受影响
	<b>ID</b>	<b>11.6(1)</b>	<b>12.0(1)</b>	<b>12.5(1)</b>	<b>12.6(1)</b>
CVP	<a href="#">CSCwa47275</a>	<a href="#">补丁 — 11.6(1)ES16 自述</a>	<a href="#">补丁 — 12.0(1) ES10 自述</a>	<a href="#">补丁 — 12.5(1) ES25 自述</a>	<a href="#">补丁 — 12.6(1) ES25 自述</a>
VVB	<a href="#">CSCwa47397</a>	不受影响	不受影响	<a href="#">补丁 — 12.5(1) ES12 自述</a>	<a href="#">补丁 — 12.6(1) ES12 自述</a> *使用2021年2月29日发布的
呼叫工作室	<a href="#">CSCwa54008</a>	<a href="#">Callstudio 11.6 L og4j fix 自述</a>	<a href="#">Callstudio 12.0(1) Log4j fix 自述</a>	<a href="#">Callstudio 12.5(1) Log4j fix 自述</a>	<a href="#">Callstudio 12.6(1) Log4j fix 自述</a>
Finesse	<a href="#">CSCwa46459</a>	不受影响	不受影响	不受影响	<a href="#">补丁 — 12.6(1) ES12 自述</a>
CUIC	<a href="#">CSCwa46525</a>	不受影响	不受影响	不受影响	<a href="#">补丁 — 12.6(1) ES12 自述</a>
实时数据(LD)	<a href="#">CSCwa46810</a>	<a href="#">补丁 — 11.6.1 COP23 自述</a>	<a href="#">补丁 — 12.0(1) ES18 自述</a>	<a href="#">补丁 — 12.5(1) ES13 自述</a>	<a href="#">补丁 — 12.6(1) ES13 自述</a>
IDS		不受影响	不受影响	不受影响	不受影响
CUIC共享(CUIC-LD-IDS)	<a href="#">CSCwa46810</a>	<a href="#">补丁 — 11.6.1 COP23 自述</a>	<a href="#">补丁 — 12.0(1) ES18 自述</a>	<a href="#">补丁 — 12.5(1) ES13 自述</a>	<a href="#">补丁 — 12.6(1) ES13 自述</a>
CloudConnect	<a href="#">CSCwa51545</a>			不受影响	<a href="#">补丁 — 12.6(1) CC 自述</a>
ECE	<a href="#">CSCwa47392</a>	不受影响	<a href="#">补丁 — 12.0(1) ES6 ET2 自述</a>	<a href="#">补丁 — 12.5(1) ES3 ET2 自述</a>	<a href="#">补丁 — 12.6(1) ES3 ET2 自述</a>
CCMP	<a href="#">CSCwa47383</a>	不受影响	不受影响	<a href="#">补丁 — 12.5(1) ES6 自述</a>	<a href="#">Patch- 12.6(1) ES6 自述</a>

[自述](#)

[补丁 — 12.6\(1\) ES6](#)  
[自述](#)

CCDM	<a href="#">CSCwa47383</a>	不受影响	不受影响	<a href="#">补丁 — 12.5(1) ES6</a> <a href="#">自述</a>	
Google CCAI	Google确认CCAI功能集未受影响				
Webex体验管理(WxM)	WxM不使用log4j，因此解决方案不受影响				
客户协作平台(CCP)	<a href="#">CSCwa47384</a>	不受影响	不受影响	不受影响	不受影响

\*发布日期可能会更改，并会根据需要更新，直到发布补丁

## ICM服务器上的Tomcat版本检查

- 1.在ICM服务器（即路由器、记录器、PG和AW服务器）上，通过运行“<ICM HOME>\tomcat\bin\version.bat”文件检查安装的tomcat的版本。
- 2.如果tomcat版本为**9.0.37或更高版本**，请执行以下步骤修复缺陷“[CSCv73307](#)”
- 3.在服务器上安装ES\_81补丁。如果ICM服务器上有大于81的ES，请确保首先卸载这些ES

- 12.5(1)\_ES81补丁 —

<https://software.cisco.com/download/specialrelease/0aab225ecde522734cc6c6491ad1eb42>

- 12.5(1)\_ES81自述 —

[https://www.cisco.com/web/software/280840583/158250/Release\\_Document\\_1.html](https://www.cisco.com/web/software/280840583/158250/Release_Document_1.html)

- 4.成功安装ES\_81后，运行bat文件“<ICM HOME>\tomcat\bin\version.bat”，再次确认tomcat版本
5. Tomcat版本应与步骤1相同，如果相同，则继续有序重新安装所有所需ES的最新和包括log4j补丁，即ES\_101

## 常见问题

问。1使用最新信息修改文档的频率如何？

答案： 文档每天审核，并在上午（美国时间）更新

问题2是ICM版本，即（路由器、记录器、AW、PG）10.x、11.0(x)、11.5(x)和11.6(1)受影响？

答案： 这些版本使用1.X版log4j时不受影响。

**注意：**顾问表列出了正在维护的版本的特定错误。未突出显示的版本将结束软件维护，不会考虑进行审核。

问。3补丁何时发布？

答案： 建议表突出显示了发布补丁的暂定日期。该表将随相关链接的可用而更新。

问。4在修复就绪之前可以实施的任何解决方法？

答案：建议遵循PSIRT建议，并确保补丁在针对受影响版本发布后尽快应用。

Q.5 CUIIC独立版11.6(1)不受log4j影响，但ES的自述文件在服务器上声明了它所需的补丁 — 为什么？

答案：此ES不是仅具有log4j修复的独立ES，此ES23是任何VOS产品都会具有的累积ES。也就是说，客户在任何时间点都只能使用一个最新的累积ES。请考虑此场景，其中Cu位于独立CUIIC 11.6 ES 21（或之前）中，并且需要ES22的CUIIC缺陷修复，在这种情况下，他们仍需要安装ES23（因为ES是累积型的，并且只有最新版本的ES可供客户使用）。此外，在ES自述文件中，此log4j缺陷已被提及并列在LD缺陷下。在ES安装期间，根据适用的部署安装缺陷修复程序（即是否进行部署检查 — 在ES安装之前是否应用独立CUIIC /co-res CUIIC/LD并相应地应用缺陷修复程序）

问。6如果我的组织使用安全扫描程序，我会采取什么操作(例如：Qualys)在我为UCCE产品打补丁后收集CVE-2021-45105？

答案：思科已审核CVE-2021-45105，并确定此漏洞不会影响思科产品或云产品，因此无需采取任何操作。该信息也已在咨询中重点介绍。要使Log4j版本2.16.0易受DDoS攻击，需要非默认配置才能获利。这意味着攻击者应手动修改log4j配置文件，这在UCCE产品中是不可能的，因此CVE-2021-45105不适用。

问题7：当我在系统上看到较旧的Log4j“.jar”文件（如1.2x文件）时，该怎么办？

答案：建议保留旧文件，以便回滚过程不会中断。在系统中拥有这些文件的非活动版本不会使组件易受攻击。

但是，如果企业需要删除文件，强烈建议在实施生产步骤之前在实验室中测试所需的流程，以最大限度地减少影响。此外，建议使用备份和回滚计划，以便在活动出现问题时恢复系统。