

CVE-2020-9480 | Apache Spark 远程代码执行漏洞通告

0x00 漏洞概述

CVE ID	CVE-2020-9480	时间	2020-06-24
类型	RCE	等级	高危
远程利用	是	影响范围	Apache Spark < = 2.4.5

0x01 漏洞详情



Apache Spark 是专为大规模数据处理而设计的快速通用的计算引擎。Apache Spark 是一种与 Hadoop 相似的开源集群计算环境，启用了内存分布数据集，除了能够提供交互式查询外，它还可以优化迭代工作负载。Apache Spark 是在 Scala 语言中实现的，它将 Scala 用作其应用程序框架。

2020 年 6 月 23 日，国家信息安全漏洞共享平台（CNVD）收录了 Apache Spark 远程代码执行漏洞。该漏洞源于 Spark 的认证机制存在缺陷，导致共享密钥认证失效。攻击者可在未授权的情况下，远程发送精心构造的过程调用指令，来启动 Spark 集群上的应用程序资源，并获得目标服务器的权限，从而实现远程代码执行。

该漏洞等级为高危，启明星辰 VSRC 建议受影响的用户及时升级至最新版本。

0x02 处置建议

官方已发布最新版本，下载地址：

<https://github.com/apache/spark/releases>

0x03 相关新闻

<https://osint.geekcq.com/2020/06/23/cve-2020-9480/>

0x04 参考链接

<https://www.cnvd.org.cn/webinfo/show/5585>

<https://github.com/apache/spark/releases>

0x05 时间线

2020-06-23 CNVD 发布通告

2020-06-24 VSRC 发布漏洞通告