Apache Hadoop 远程代码执行漏洞（CVE-2022-25168）通告

■ 通告编号 **NS-2022-00**	■ 发布日期 **2022-08-05**
■ 漏洞危害 攻击者利用此漏洞，可实现远程命令执行。	
■ **TAG** Apache Hadoop、CVE-2022-25168	

© 2022 绿盟科技

一. 漏洞概述

近日，绿盟科技 CERT 监测发现 Apache Hadoop 官方修复了一个命令注入漏洞。由于 Apache Hadoop 的 FileUtil.unTar API 在传递 shell 之前未对输入的文件名进行转义，攻击者可以利用该漏洞注入任意命令，从而实现远程代码执行。请受影响的用户采取措施进行防护。

Hadoop 是 Apache 基金会旗下的一个开源的分布式计算平台，基于 Java 语言开发，有很好的跨平台特性，并且可以部署在廉价的计算机集群中。用户无需了解分布式底层细节，就可以开发分布式程序，充分利用集群的威力进行高速运算和存储。

参考链接：https://www.mail-archive.com/announce@apache.org/msg07488.html

二. 影响范围

受影响版本

- 2.0.0 <= Apache Hadoop <= 2.10.1
- 3.0.0-alpha <= Apache Hadoop <= 3.2.3
- 3.3.0 <= Apache Hadoop <= 3.3.2

不受影响版本

- Apache Hadoop 2.10.2
- Apache Hadoop 3.2.4
- Apache Hadoop 3.3.3

三. 漏洞防护

3.1 官方升级

目前官方已在最新版本中修复了该漏洞，请受影响的用户尽快安装更新进行防护，官方下载链接：https://hadoop.apache.org/

© 2022 绿盟科技

声明

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。

绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。

© 2022 绿盟科技

密级：公开使用