**漏洞报告**

漏洞编号: CVE-2020-9492

漏洞描述: 在 Apache Hadoop 3.2.0 到 3.2.1、3.0.0-alpha1 到 3.1.3 和 2.0.0-alpha 到 2.10.0 中，WebHDFS 客户端可能会在没有正确验证的情况下将 SPNEGO 授权标头发送到远程 URL。

漏洞来源:

平台: CVE/NVD

链接: <https://nvd.nist.gov/vuln/detail/CVE-2020-9492>

漏洞披露时间: 01/26/2021

漏洞参考链接:

链接: <https://bugzilla.redhat.com/show_bug.cgi?id=1925237>

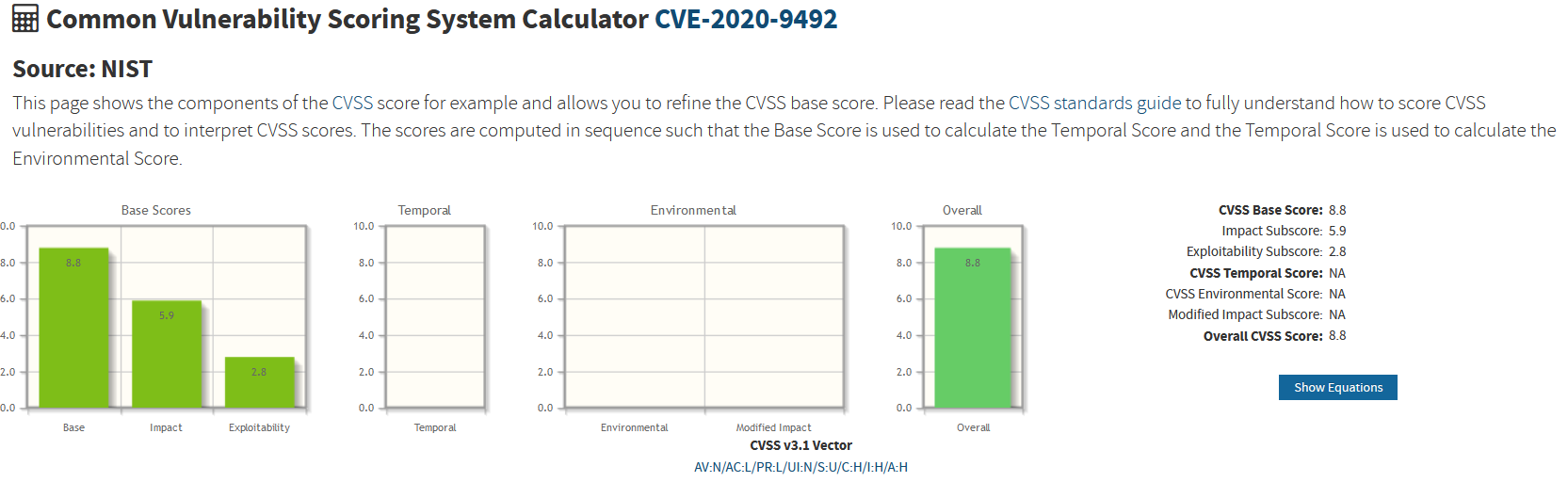
野外漏洞报告：

报告链接: <https://www.venustech.com.cn/new_type/aqtg/20210127/22338.html>

漏洞类型: 权限提升漏洞

漏洞危害: 可能会导致绕过权限机制，导致权限提升漏洞。

CVSS评分: 8.8 (已检验)



漏洞影响的组件版本:

Apache hadoop 2.0.0 - 2.10.0 (已在其他报告中验证)

Apache hadoop 3.0.0 - 3.1.3 (已在其他报告中验证)

Apache hadoop 3.2.0 - 3.2.1 (已在其他报告中验证)

Apache solr 8.6.0

Apache solr 8.6.2

Oracle financial\_services\_crime\_and\_compliance\_management\_studio 8.0.8.2.0 , 8.0.8.3.0

漏洞修复的组件版本:

Apache hadoop 2.10.1

Apache hadoop 3.1.4

Apache hadoop 3.2.2

漏洞成因:

在Apache hadoop中发现一个缺陷。WebHDFS客户端可以向远程URL发送SPNEGO授权头，而不需要适当的验证，这可能导致访问限制的绕过。这个漏洞的最大威胁是数据的保密性和完整性以及系统的可用性。

漏洞位置:

根据补丁可以看出: 漏洞具体位置在hadoop-hdfs-project/hadoop-hdfs-client/src/main/java/org/apache/hadoop/hdfs/web/WebHdfsFileSystem.java文件中

漏洞PoC: N/A

漏洞补丁:

参考链接: <https://github.com/apache/hadoop/commit/81d8a887b0406380e469c76ed2e41022a6372dd7>

漏洞处置建议：

1. 设置不同的http签名机密，并使用专用主机进行每个权限模拟服务（如HiveServer2）。

2. 升级到3.3.0、3.2.2、3.1.4、2.10.1或更新的TLS加密版本，启用并将dfs.http.policy配置为HTTPS\_ONLY。