**漏洞报告**

漏洞编号: CVE-2021- 20180

漏洞描述: 在 ansible 模块中发现了一个缺陷，默认情况下，凭据在控制台日志中公开，并且在使用 bitbucket\_pipeline\_variable 模块时不受安全功能的保护。此缺陷允许攻击者窃取 bitbucket\_pipeline 凭据。此漏洞的最大威胁是与机密性有关。

漏洞来源:

平台: CVE/NVD

链接: <https://nvd.nist.gov/vuln/detail/CVE-2021-20180>

漏洞披露时间: 03/16/2022

漏洞参考链接: 见下面的链接

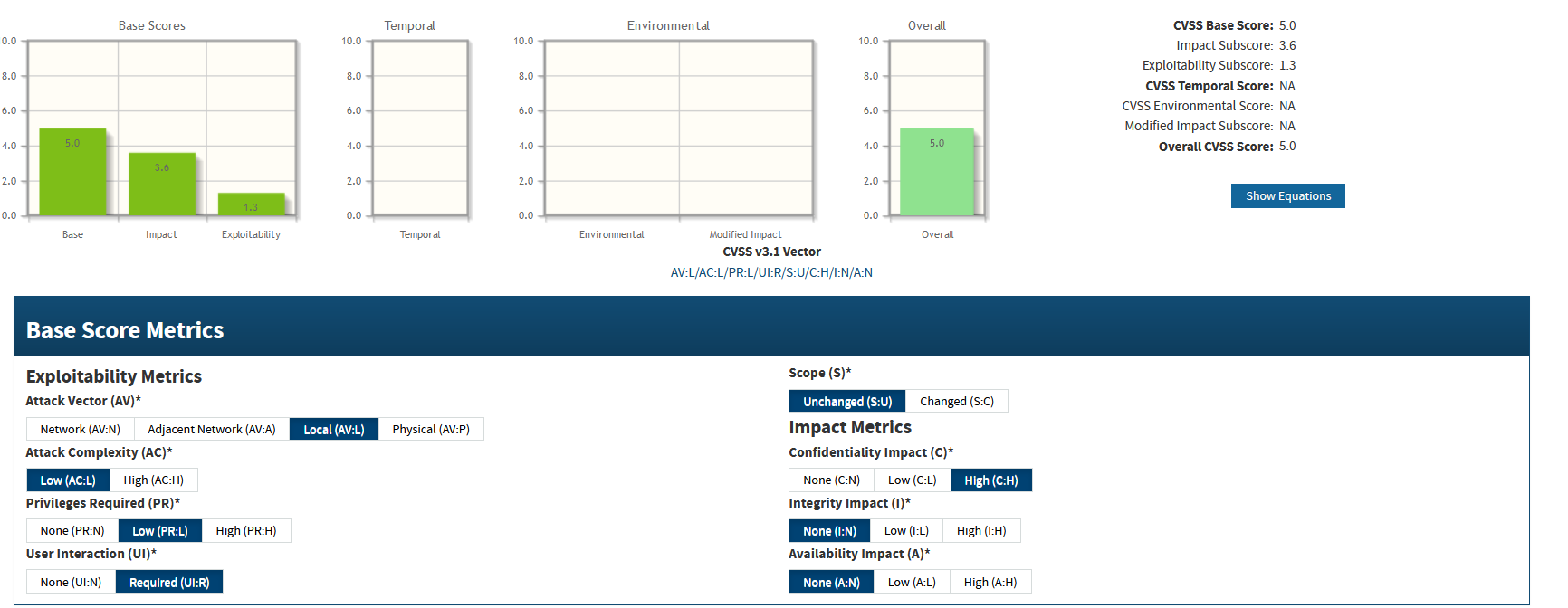
野外漏洞报告：N/A

漏洞类型: 本地类型攻击漏洞

漏洞危害:

CVSS评分: 5.5 (NVD评分)

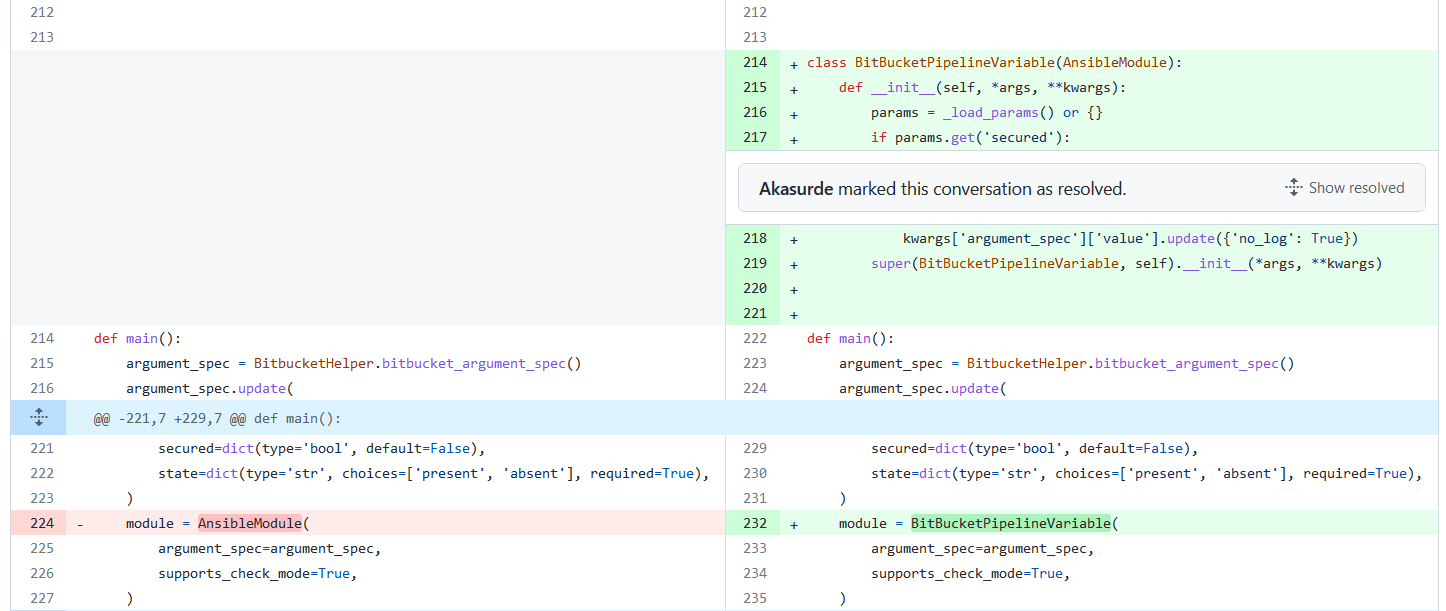
重新评价后: 5.0



漏洞影响的组件版本:

Redhat ansible 2.9.18之前的版本

经过验证，在2.9.18版本加入了隐藏标记为安全的用户敏感信息的代码：



在之前的版本都没有，详细代码见漏洞补丁一栏。

漏洞修复的组件版本: 2.9.18

漏洞成因:

默认情况下，凭据在控制台日志中公开，并且在使用 bitbucket\_pipeline\_variable 模块时不受安全功能的保护。此缺陷允许攻击者窃取 bitbucket\_pipeline 凭据。Red Hat Gluster Storage 3 中提供的 Ansible 版本不包含易受攻击的 bitbucket 模块，不受此漏洞影响。但是，Red Hat Gluster Storage 3 不再维护自己的 Ansible 版本。先决条件是启用 Ansible 存储库，以便使用最新版本的 Ansible，其中包括错误和安全修复。具体相关的代码可在漏洞补丁中查看。

漏洞位置:

bitbucket\_pipeline\_variable 模块中，根据补丁可以得出漏洞具体位置在plugins/modules/source\_control/bitbucket/bitbucket\_pipeline\_variable.py文件中

漏洞PoC：N/A

漏洞补丁：

链接:

<https://github.com/ansible-collections/community.general/pull/1635/commits/8de555b5d69debb9bbed877922024385718edd3f>

备注: bitbucket\_pipeline\_variable - 隐藏标记为安全的用户敏感信息以防止登录控制台。

漏洞处置建议：

参考链接: <https://access.redhat.com/errata/RHSA-2021:2180>

将Redhat ansible更新到2.9.18+