



# CVE-2021-20180

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#) 

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2021-20180  |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | secalert@redhat.com   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2022-03-16 15:15:00 UTC   |
| <b>Updated</b>         | 2022-03-22 15:43:00 UTC   |
| <b>Description</b>     | A flaw was found in ansible module where credentials are disclosed in the console log by default and not protected by the s |

## Risk And Classification

**Problem Types:** CWE-532

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|---------|---------|--------|---------|----------|
| Application | Redhat | Ansible | All     | All    | All     | All      |

## References

| Reference  | Source  | Link                      |
|--|---------|---------------------------|
| 1915808 – (CVE-2021-20180) CVE-2021-20180 ansible module: bitbucket_pipeline_variable exposes secured values | MISC    | <a href="#">bugzilla.</a> |
| CVE Program record   | CVE.ORG | <a href="#">www.cve</a>   |
| NVD vulnerability detail   | NVD     | <a href="#">nvd.nist.</a> |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

|  |
|--|
| <a href="#">183474</a> Debian Security Update for ansible (CVE-2021-20180)                     |
| <a href="#">239447</a> Red Hat Update for RHV Engine and Host Common Packages (RHSA-2021:2180) |
| <a href="#">281605</a> Fedora Security Update for ansible (FEDORA-2021-9a0903469c)             |
| <a href="#">281606</a> Fedora Security Update for ansible (FEDORA-2021-e9478617ae)             |
| <a href="#">352253</a> Amazon Linux Security Advisory for ansible: ALAS2-2021-1613             |

[356209](#) Amazon Linux Security Advisory for ansible : ALASANSIBLE2-2023-004

[356466](#) Amazon Linux Security Advisory for ansible : ALAS2ANSIBLE2-2023-004

[752570](#) SUSE Enterprise Linux Important for SUSE Manager Client Tools (SUSE-SU-2022:3178-1)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**