



CVE-2021-20178

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

Summary

CVE	CVE-2021-20178
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-26 12:15:00 UTC
Updated	2023-12-28 19:15:00 UTC
Description	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
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Redhat	Ansible	All	All	All	All
Application	Redhat	Ansible Tower	3.0	All	All	All

References

Reference	Source	Link	Tag
[SECURITY] Fedora 33 Update: ansible-2.9.18-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
ansible/CHANGELOG-v2.9.rst at v2.9.18 · ansible/ansible · GitHub	MISC	github.com	
[SECURITY] [DLA 3695-1] ansible security update		lists.debian.org	
[SECURITY] Fedora 32 Update: ansible-2.9.18-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
ansible/CHANGELOG-v2.9.rst at v2.9.18 · ansible/ansible · GitHub		github.com	
1914774 – (CVE-2021-20178) CVE-2021-20178 ansible: user data leak in snmp_facts module	MISC	bugzilla.redhat.com	
github.com/ansible-collections/community.general/pull/1635%2C		github.com	
[SECURITY] Fedora 32 Update: ansible-2.9.18-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 33 Update: ansible-2.9.18-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
github.com/ansible-collections/community.general/pull/1635,	MISC	github.com	

CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [184886](#) Debian Security Update for ansible (CVE-2021-20178)
- [239447](#) Red Hat Update for RHV Engine and Host Common Packages (RHSA-2021:2180)
- [281605](#) Fedora Security Update for ansible (FEDORA-2021-9a0903469c)
- [281606](#) Fedora Security Update for ansible (FEDORA-2021-e9478617ae)
- [352253](#) 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
- [6000405](#) Debian Security Update for ansible (DLA 3695-1)
- [752570](#) SUSE Enterprise Linux Important for SUSE Manager Client Tools (SUSE-SU-2022:3178-1)
- [900111](#) CBL-Mariner Linux Security Update for ansible 2.9.12
- [903566](#) Common Base Linux Mariner (CBL-Mariner) Security Update for ansible (4264)
- [982362](#) Python (pip) Security Update for ansible (GHSA-wv5p-gmmv-wh9v)

© [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](#)