CVE-2021-3620

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-3620
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-03 19:15:00 UTC
Updated	2023-12-28 19:15:00 UTC
Description	A flaw was found in Ansible Engine's ansible-connection module, where sensitive information such as the Ansible user cred

Risk And Classification

Problem Types: CWE-209

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Ansible Automation Platform Early Access	2.0	All	All	All
Application	Redhat	Ansible Engine	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	8.0	All	All	All
Application	Redhat	Openstack	1	All	All	All
Application	Redhat	Openstack	16.1	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All
Application	Redhat	Virtualization For Ibm Power Little Endian	4.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All
Application	Redhat	Virtualization Manager	4.4	All	All	All

References

Reference	Sour
[SECURITY] [DLA 3695-1] ansible security update	
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
ansible/CHANGELOG-v2.9.rst at stable-2.9 · ansible/ansible · GitHub	MISC

Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
Fixed exposed credentials in exception · ansible/ansible@fe28767 · GitHub	MISC
1975767 – (CVE-2021-3620) CVE-2021-3620 Ansible: ansible-connection module discloses sensitive info in traceback error message	MISC
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 182689 Debian Security Update for ansibleansible-core (CVE-2021-3620)
- 239679 Red Hat Update for Ansible (RHSA-2021:3872)
- 239680 Red Hat Update for Ansible (RHSA-2021:3871)
- 239893 Red Hat Update for rhv engine and host common packages (RHSA-2021:4703)
- 282037 Fedora Security Update for ansible (FEDORA-2021-0e7910e389)
- 282038 Fedora Security Update for ansible (FEDORA-2021-71ff867094)
- 6000405 Debian Security Update for ansible (DLA 3695-1)
- 690196 Free Berkeley Software Distribution (FreeBSD) Security Update for ansible (9a8514f3-2ab8-11ec-b3a1-8c164582fbac)
- 752570 SUSE Enterprise Linux Important for SUSE Manager Client Tools (SUSE-SU-2022:3178-1)
- 900748 Common Base Linux Mariner (CBL-Mariner) Security Update for ansible (8942)
- 902007 Common Base Linux Mariner (CBL-Mariner) Security Update for ansible (8942-1)