



# CVE-2020-25635

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-25635
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-10-05 14:15:00 UTC
<b>Updated</b>	2023-11-07 03:20:00 UTC
<b>Description</b>	A flaw was found in Ansible Base when using the aws_ssm connection plugin as garbage collector is not happening after pl

## Risk And Classification

**Problem Types:** CWE-212

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Ansible	2.10.1	rc2	All	All
Application	Redhat	Ansible	2.10.1	rc2	All	All

## References

### Reference

- 1880275 – (CVE-2020-25635) CVE-2020-25635 Collections: aws\_ssm connection plugin should garbage collect the s3 bucket after the file tra
- aws\_ssm connection plugin should garbage collect the s3 bucket after the file transfers · Issue #222 · ansible-collections/community.aws · GitH
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[691129](#) Free Berkeley Software Distribution (FreeBSD) Security Update for py (e1b77733-a982-442e-8796-a200571bfcf2)

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](#).

**Free CVE JSON API** [cve.report/api](#)

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