



# CVE-2023-39059

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

## Summary

|                        |                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2023-39059                                                                                                               |
| <b>State</b>           | PUBLIC                                                                                                                       |
| <b>Assigner</b>        | cve@mitre.org                                                                                                                |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                 |
| <b>Published</b>       | 2023-08-28 22:15:00 UTC                                                                                                      |
| <b>Updated</b>         | 2023-08-30 00:30:00 UTC                                                                                                      |
| <b>Description</b>     | An issue in ansible semaphore v.2.8.90 allows a remote attacker to execute arbitrary code via a crafted payload to the extra |

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor            | Product           | Version | Update | Edition | Language |
|-------------|-------------------|-------------------|---------|--------|---------|----------|
| Application | Ansible-semaphore | Ansible Semaphore | 2.8.90  | All    | All     | All      |

## References

| Reference                                                                     | Source  | Link                                                  | Tags                |
|-------------------------------------------------------------------------------|---------|-------------------------------------------------------|---------------------|
| CVE-2023-39059 · GitHub                                                       | MISC    | <a href="https://gist.github.com">gist.github.com</a> |                     |
| A Quick Story Of Security Pitfalls With Exec.Command In Software Integrations | MISC    | <a href="https://www.alevsk.com">www.alevsk.com</a>   |                     |
| CVE Program record                                                            | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>         | canonical           |
| NVD vulnerability detail                                                      | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>       | canonical, analysis |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)