



# CVE-2023-41882

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

## Summary

<b>CVE</b>	CVE-2023-41882
<b>State</b>	PUBLIC
<b>Assigner</b>	security-advisories@github.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-10-11 20:15:00 UTC
<b>Updated</b>	2023-10-18 02:27:00 UTC
<b>Description</b>	vantage6 is privacy preserving federated learning infrastructure. The endpoint /api/collaboration/{id}/task is used to collect a

## Risk And Classification

**Problem Types:** CWE-284

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vantage6	Vantage6	All	All	All	All

## References

Reference	Source	Link	Tags
Improper Access Control in vantage6 · Advisory · vantage6/vantage6 · GitHub	MISC	<a href="https://github.com">github.com</a>	
Feature/collaboration scope by bartvanb · Pull Request #711 · vantage6/vantage6 · GitHub	MISC	<a href="https://github.com">github.com</a>	
Release notes	MISC	<a href="https://github.com">github.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.

## Legacy QID Mappings

995574 Python (Pip) Security Update for vantage6 (GHSA-gc57-xhh5-m94r)

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](#)