



# CVE-2023-0164

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

## Summary

<b>CVE</b>	CVE-2023-0164
<b>State</b>	PUBLIC
<b>Assigner</b>	help@fluidattacks.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-01-18 22:15:00 UTC
<b>Updated</b>	2023-01-28 03:37:00 UTC
<b>Description</b>	OrangeScrum version 2.0.11 allows an authenticated external attacker to execute arbitrary commands on the server. This is

## Risk And Classification

**Problem Types:** CWE-78

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Orangescrum	Orangescrum	2.0.11	All	All	All

## References

### Reference

- OrangeScrum 2.0.11 - OS Command Injection via projuniqid | Advisories | Fluid Attacks
- GitHub - Orangescrum/orangescrum: Orangescrum is a simple yet powerful free and open source project management software that helps tea
- CVE Program record
- NVD vulnerability detail

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)