



# CVE-2023-28367

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

## Summary

<b>CVE</b>	CVE-2023-28367
<b>State</b>	PUBLIC
<b>Assigner</b>	vultures@jpcert.or.jp
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-05-23 02:15:00 UTC
<b>Updated</b>	2023-05-30 15:55:00 UTC
<b>Description</b>	Cross-site scripting vulnerability in CTA post function of VK All in One Expansion Unit 9.88.1.0 and earlier allows a remote e

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vektor-inc	Vk All In One Expansion Unit	All	All	All	All

## References

Reference	Source	Link
VK Blocks / ExUnit の脆弱性について   株式会社ベクトル	MISC	<a href="http://www.vektor.jp">www.vektor.jp</a>
JVN#95792402: WordPress Plugin "VK Blocks" and "VK All in One Expansion Unit" vulnerable to cross-site scripting	MISC	<a href="http://jvn.jp">jvn.jp</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

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)