



# CVE-2021-46364

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

## Summary

<b>CVE</b>	CVE-2021-46364
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-02-11 21:15:00 UTC
<b>Updated</b>	2022-03-29 16:08:00 UTC
<b>Description</b>	A vulnerability in the Snake YAML parser of Magnolia CMS v6.2.3 and below allows attackers to execute arbitrary code via

## Risk And Classification

**Problem Types:** CWE-502

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Magnolia-cms	Magnolia Cms	All	All	All	All

## References

Reference	Source	Link
Disclosures/CVE-2021-46364-YAML Deserialization-Magnolia CMS at master · DrunkenShells/Disclosures · GitHub	MISC	<a href="#">github.com</a>
Release notes for Magnolia CMS 6.2.4 :: Magnolia CMS Docs	MISC	<a href="#">docs.magnolia-cms.com</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">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)