



# CVE-2023-38836

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

## Summary

<b>CVE</b>	CVE-2023-38836
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-08-21 17:15:00 UTC
<b>Updated</b>	2023-10-10 17:15:00 UTC
<b>Description</b>	File Upload vulnerability in BoidCMS v.2.0.0 allows a remote attacker to execute arbitrary code by adding a GIF header to k

## Risk And Classification

**Problem Types:** CWE-434

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Boidcms	Boidcms	2.0.0	All	All	All

## References

### Reference

BoidCMS 2.0.0 Shell Upload ≈ Packet Storm

boidcms.com

[VULNERABILITY] Authenticated file upload vulnerability - [leading to shell command execution] · Issue #27 · BoidCMS/BoidCMS · GitHub

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.

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

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