



# CVE-2026-30625

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

## Summary

<b>CVE</b>	CVE-2026-30625
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-15 16:16:36 UTC
<b>Updated</b>	2026-04-15 16:16:36 UTC
<b>Description</b>	Upsonic 0.71.6 contains a remote code execution vulnerability in its MCP server/task creation functionality. The application

## Risk And Classification

**Problem Types:** n/a

## Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

## References

Reference	Source	Link	Tags
github.com/Upsonic/Upsonic/commit/855053fce0662227d9246268ff4a0844b481a305	cve@mitre.org	<a href="#">github.com</a>	
www.ox.security/blog/mcp-supply-chain-advisory-rce-vulnerabilities-across-the...	cve@mitre.org	<a href="#">www.ox.security</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analys

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)