



# CVE-2012-6649

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

## Summary

<b>CVE</b>	CVE-2012-6649
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-01-23 22:15:00 UTC
<b>Updated</b>	2020-01-29 17:44:00 UTC
<b>Description</b>	WordPress WP GPX Maps Plugin 1.1.21 allows remote attackers to execute arbitrary PHP code via improper file upload.

## Risk And Classification

**Problem Types:** CWE-434

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Devfarm</a>	<a href="#">Wp Gpx Maps</a>	1.1.21	All	All	All
Application	<a href="#">Devfarm</a>	<a href="#">Wp Gpx Maps</a>	1.1.21	All	All	All

## References

### Reference

- WordPress WP GPX Maps Plugin Arbitrary File Upload Vulnerability
- oss-security - Re: CVE request: WordPress plugin wp-gpx-maps wp-gpx-maps\_admin\_tracks.php Improper Admin Verification File Upload PH
- 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.

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)