# CVE Detail – CVE-2012-0911

TikiWiki CMS/Groupware before 6.7 LTS and before 8.4 allows remote attackers to execute arbitrary PHP code via a crafted serialized object in the (1) cookieName to lib/banners/bannerlib.php; (2) printpages or (3) printstructures parameter to (a) tiki-print\_multi\_pages.php or (b) tiki-print\_pages.php; or (4) sendpages, (5) sendstructures, or (6) sendarticles parameter to tiki-send\_objects.php, which is not properly handled when processed by the unserialize function.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.98945

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* CWE-502: Deserialization of Untrusted Data

## CAPEC(s)

* CAPEC-586: Object Injection

## Affected Products

* cpe:2.3:a:tiki:tikiwiki\_cms\/groupware:\*:\*:\*:\*:lts:\*:\*:\*
* cpe:2.3:a:tiki:tikiwiki\_cms\/groupware:\*:\*:\*:\*:-:\*:\*:\*