



# CVE-2017-8102

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

## Summary

<b>CVE</b>	CVE-2017-8102
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-04-24 18:59:00 UTC
<b>Updated</b>	2017-04-28 15:57:00 UTC
<b>Description</b>	Stored XSS in Serendipity v2.1-rc1 allows an attacker to steal an admin's cookie and other information by composing a new

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	S9y	Serendipity	2.1	rc1	All	All
Application	S9y	Serendipity	2.1	rc1	All	All

## References

Reference	Source
stored XSS in v2.1-rc1 · Issue #456 · s9y/Serendipity · GitHub	MISC
Full Disclosure: CVE-Request:stored XSS in Serendipity v2.1-rc1 allows attacker steals admin's cookie and other informations	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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)