



# CVE-2016-9681

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

## Summary

<b>CVE</b>	CVE-2016-9681
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-12-25 17:59:00 UTC
<b>Updated</b>	2016-12-30 19:57:00 UTC
<b>Description</b>	Multiple cross-site scripting (XSS) vulnerabilities in Serendipity before 2.0.5 allow remote authenticated users to inject arbitrary HTML and JavaScript into pages. An attacker could then inject arbitrary HTML and JavaScript into pages. This could allow an attacker to hijack sessions, steal sensitive information, and perform actions on behalf of the user.

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

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

## References

Reference	Source	Link	Tags
Sync changes · s9y/Serendipity@e2a665e · GitHub	MISC	<a href="https://github.com">github.com</a>	Patch, Vendor Advisory
Serendipity 'serendipity_admin.php' Multiple Cross Site Scripting Vulnerabilities	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Third Party Advisory
Edric Teo	MISC	<a href="http://smarterbitbybit.com">smarterbitbybit.com</a>	Exploit, Technical Details
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

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)