



# CVE-2014-9229

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

## Summary

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2014-9229                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>State</b>           | PUBLIC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Assigner</b>        | secure@symantec.com                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Published</b>       | 2015-09-20 20:59:00 UTC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Updated</b>         | 2017-09-23 01:29:00 UTC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Description</b>     | Multiple SQL injection vulnerabilities in interface PHP scripts in the Manager component in Symantec Endpoint Protection (SEP) 14.0.0.100 and 14.0.0.110 allow an attacker to inject arbitrary SQL commands and execute them as the user running the SEP Manager service. This vulnerability is caused by a lack of input validation in the PHP scripts. The attack can be performed remotely and does not require authentication. The impact is that an attacker can execute arbitrary SQL commands and potentially gain access to sensitive data or escalate their privileges. The vulnerability is present in the Manager component, which is responsible for managing the SEP client. The attack is performed by sending a specially crafted HTTP request to the Manager component. The request contains a SQL injection payload that is executed by the database. The database returns the results of the query to the Manager component, which then displays them to the user. The user can see the results of the query, which may include sensitive data. The vulnerability is present in the Manager component, which is responsible for managing the SEP client. The attack is performed by sending a specially crafted HTTP request to the Manager component. The request contains a SQL injection payload that is executed by the database. The database returns the results of the query to the Manager component, which then displays them to the user. The user can see the results of the query, which may include sensitive data. |

## Risk And Classification

### Problem Types: CWE-89

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                   | Product                             | Version | Update | Edition | Language |
|-------------|--------------------------|-------------------------------------|---------|--------|---------|----------|
| Application | <a href="#">Symantec</a> | <a href="#">Endpoint Protection</a> | All     | All    | All     | All      |

## References

| Reference                                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Symantec Endpoint Protection Manager and Client CVE-2014-9229 SQL Injection Vulnerability</a>                                                       |
| <a href="#">Security Advisories Relating to Symantec Products - Symantec Endpoint Protection Manager and Client Issues - 2015-06-17T00:00:00 PDT   Symantec</a> |
| <a href="#">Symantec Endpoint Protection Lets Remote Authenticated Users Inject SQL Commands and Local Users Deny Service and Gain Elevated Privileges</a>      |
| <a href="#">CVE Program record</a>                                                                                                                              |
| <a href="#">NVD vulnerability detail</a>                                                                                                                        |

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)