# CVE-2014-9230

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2014-9230 |
| **State** | PUBLIC |
| **Assigner** | secure@symantec.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2015-06-28 19:59:00 UTC |
| **Updated** | 2017-09-22 01:29:00 UTC |
| **Description** | Cross-site scripting (XSS) vulnerability in the administration console in the Enforce Server in Symantec Data Loss Preventic |

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Symantec | Data Loss Prevention | All | All | All | All |

## References

| Reference |
|---|
| Symantec Data Loss Prevention CVE-2014-9230 Multiple HTML Injection Vulnerabilities |
| Security Advisories Relating to Symantec Products - Symantec Data Loss Prevention Enforce Server Administration Console Cross-site Script |
| Symantec Data Loss Prevention Enforce Server Input Validation Flaws Permit Cross-Site Scripting and Cross-Site Request Forgery Attacks - |
| 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.

**CVE.report and Source URL Uptime Status status.cve.report**