



# CVE-2014-3438

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

## Summary

|                        |                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2014-3438                                                                                                                |
| <b>State</b>           | PUBLIC                                                                                                                       |
| <b>Assigner</b>        | secure@symantec.com                                                                                                          |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                 |
| <b>Published</b>       | 2014-11-07 11:55:00 UTC                                                                                                      |
| <b>Updated</b>         | 2018-10-09 19:43:00 UTC                                                                                                      |
| <b>Description</b>     | Multiple cross-site scripting (XSS) vulnerabilities in console interface scripts in Symantec Endpoint Protection Manager (SE |

## Risk And Classification

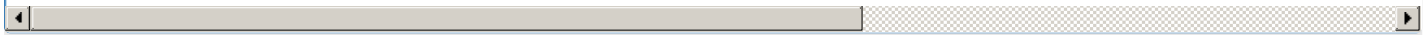
### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                   | Product                                     | Version | Update | Edition | Language |
|-------------|--------------------------|---------------------------------------------|---------|--------|---------|----------|
| Application | <a href="#">Symantec</a> | <a href="#">Endpoint Protection Manager</a> | 12.1.0  | All    | All     | All      |
| Application | <a href="#">Symantec</a> | <a href="#">Endpoint Protection Manager</a> | 12.1.1  | All    | All     | All      |
| Application | <a href="#">Symantec</a> | <a href="#">Endpoint Protection Manager</a> | 12.1.2  | All    | All     | All      |
| Application | <a href="#">Symantec</a> | <a href="#">Endpoint Protection Manager</a> | 12.1.3  | All    | All     | All      |
| Application | <a href="#">Symantec</a> | <a href="#">Endpoint Protection Manager</a> | 12.1.0  | All    | All     | All      |
| Application | <a href="#">Symantec</a> | <a href="#">Endpoint Protection Manager</a> | 12.1.1  | All    | All     | All      |
| Application | <a href="#">Symantec</a> | <a href="#">Endpoint Protection Manager</a> | 12.1.2  | All    | All     | All      |
| Application | <a href="#">Symantec</a> | <a href="#">Endpoint Protection Manager</a> | 12.1.3  | All    | All     | All      |
| Application | <a href="#">Symantec</a> | <a href="#">Endpoint Protection Manager</a> | All     | All    | All     | All      |

## References

| Reference                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------|
| Full Disclosure: SEC Consult SA-20141106-0 :: XXE & XSS & Arbitrary File Write vulnerabilities in Symantec Endpoint Protection              |
| IBM X-Force Exchange                                                                                                                        |
| Symantec Endpoint Protection Manager Bugs Permit Cross-Site Scripting, XML External Entity Injection, and File Overwrite Attacks - Security |
| Security Advisories Relating to Symantec Products - Symantec Endpoint Protection Manager Multiple Issues - 2014-11-05T06:00:00 PST   Sy     |
| SecurityFocus                                                                                                                               |

|                                                                                   |
|-----------------------------------------------------------------------------------|
| Malformed Request                                                                 |
| 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](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)