



# CVE-2015-8149

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

## Summary

<b>CVE</b>	CVE-2015-8149
<b>State</b>	PUBLIC
<b>Assigner</b>	secure@symantec.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-02-18 22:59:00 UTC
<b>Updated</b>	2016-12-06 03:03:00 UTC
<b>Description</b>	The LDAP service in Symantec Encryption Management Server (SEMS) 3.3.2 before MP12 allows remote attackers to cau

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Symantec	Encryption Management Server	All	mp11	All	All

## References

### Reference

- Symantec Encryption Management Server Bugs Let Remote and Local Users Gain Elevated Privileges and Remote Users Deny Service and
- Security Advisories Relating to Symantec Products - Symantec Encryption Management Server Multiple Security Issues - 2016-02-18T04:00:00
- Symantec Encryption Management Server CVE-2015-8149 Denial of Service Vulnerability
- 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.

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)