



# CVE-2015-8799

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2015-8799  |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | secure@symantec.com  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2016-06-08 14:59:00 UTC  |
| <b>Updated</b>         | 2021-09-09 17:06:00 UTC  |
| <b>Description</b>     | Directory traversal vulnerability in the Management Server in Symantec Embedded Security: Critical System Protection (SE |

## Risk And Classification

**Problem Types:** CWE-22

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor   | Product   | Version | Update |
|------------------|----------|---|---------|--------|
| Application      | Broadcom | Symantec Critical System Protection   | All     | All    |
| Application      | Broadcom | Symantec Data Center Security Server  | All     | All    |
| Application      | Broadcom | Symantec Data Center Security Server  | 6.5.0   | -      |
| Application      | Broadcom | Symantec Data Center Security Server  | 6.6.0   | All    |
| Application      | Broadcom | Symantec Data Center Security Server And Agents                                   | 6.6.0   | All    |
| Operating System | Broadcom | Symantec Embedded Security Critical System Protection                             | All     | All    |
| Operating System | Broadcom | Symantec Embedded Security Critical System Protection For Controllers And Devices | 6.5.0   | All    |
| Application      | Symantec | Critical System Protection  | All     | All    |
| Application      | Symantec | Data Center Security Server   | All     | All    |
| Application      | Symantec | Data Center Security Server   | 6.5.0   | -      |
| Application      | Symantec | Data Center Security Server   | 6.6.0   | All    |
| Application      | Symantec | Data Center Security Server   | All     | All    |
| Application      | Symantec | Data Center Security Server   | 6.5.0   | -      |
| Application      | Symantec | Data Center Security Server   | 6.6.0   | All    |
| Application      | Symantec | Data Center Security Serverand Agents   | 6.6.0   | All    |
| Application      | Symantec | Data Center Security Serverand Agents   | 6.6.0   | All    |
| Operating System | Symantec | Symantec Embedded Security Critical System Protection                             | All     | All    |

|                  |                          |   |       |     |
|------------------|--------------------------|---|-------|-----|
| Operating System | <a href="#">Symantec</a> | <a href="#">Symantec Embedded Security Critical System Protection For Controllers And Devices</a> | 6.5.0 | All |
| Operating System | <a href="#">Symantec</a> | <a href="#">Symantec Embedded Security Critical System Protection For Controllers And Devices</a> | 6.5.0 | All |

## References

| Reference  |
|--|
| <a href="#">Security Advisories Relating to Symantec Products - Symantec Embedded Security: Critical System Protection and Symantec Data Center Se</a> |
| <a href="#">Multiple Symantec Products CVE-2015-8799 Binary Planting Vulnerability</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.

© [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](#).

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