# CVE-2016-5312

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2016-5312 |
| **State** | PUBLIC |
| **Assigner** | secure@symantec.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2017-04-14 18:59:00 UTC |
| **Updated** | 2017-04-22 14:16:00 UTC |
| **Description** | Directory traversal vulnerability in the charting component in Symantec Messaging Gateway before 10.6.2 allows remote au |

## Risk And Classification

**Problem Types:** CWE-22

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Symantec | Messaging Gateway | All | All | All | All |

## References

| Reference |
|---|
| Symantec Messaging Gateway 10.6.1 Directory Traversal ≈ Packet Storm |
| Symantec Messaging Gateway CVE-2016-5312 Directory Traversal Vulnerability |
| Full Disclosure: Symantec Messaging Gateway <= 10.6.1 Directory Traversal |
| Symantec Messaging Gateway Flaw in Charting Component Lets Remote Authenticated Users View Files on the Target System - SecurityTra |
| Security Advisories Relating to Symantec Products - Symantec Messaging Gateway Security Update - 2016-09-27T09:48:18 PDT \| Symantec |
| Symantec Messaging Gateway 10.6.1 - Directory Traversal - Java webapps Exploit |
| 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 registred 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**