



CVE-2016-3646

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2016-3646 |
| State | PUBLIC |
| Assigner | secure@symantec.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2016-06-30 23:59:00 UTC |
| Updated | 2020-05-11 19:23:00 UTC |
| Description | The AntiVirus Decomposer engine in Symantec Advanced Threat Protection (ATP); Symantec Data Center Security:Server |

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|----------|-----------------------------|---------|--------|---------|----------|
| Application | Symantec | Advanced Threat Protection | All | All | All | All |
| Application | Symantec | Csapi | All | All | All | All |
| Application | Symantec | Data Center Security Server | 6.0 | All | All | All |
| Application | Symantec | Data Center Security Server | 6.0 | mp1 | All | All |
| Application | Symantec | Data Center Security Server | 6.5 | All | All | All |
| Application | Symantec | Data Center Security Server | 6.5 | mp1 | All | All |
| Application | Symantec | Data Center Security Server | 6.6 | All | All | All |
| Application | Symantec | Data Center Security Server | 6.6 | mp1 | All | All |
| Application | Symantec | Data Center Security Server | 6.0 | All | All | All |
| Application | Symantec | Data Center Security Server | 6.0 | mp1 | All | All |
| Application | Symantec | Data Center Security Server | 6.5 | All | All | All |
| Application | Symantec | Data Center Security Server | 6.5 | mp1 | All | All |
| Application | Symantec | Data Center Security Server | 6.6 | All | All | All |
| Application | Symantec | Data Center Security Server | 6.6 | mp1 | All | All |
| Application | Symantec | Endpoint Protection | 12.1.6 | All | All | All |
| Application | Symantec | Endpoint Protection | 12.1.6 | mp1 | All | All |
| Application | Symantec | Endpoint Protection | 12.1.6 | mp2 | All | All |

| | | | | | | |
|-------------|----------|---------------------------------------|--------|-----|-----|-----|
| Application | Symantec | Endpoint Protection | 12.1.6 | mp3 | All | All |
| Application | Symantec | Endpoint Protection | 12.1.6 | mp4 | All | All |
| Application | Symantec | Endpoint Protection | 12.1.6 | mp4 | All | All |
| Application | Symantec | Endpoint Protection | 12.1.6 | mp4 | All | All |
| Application | Symantec | Endpoint Protection | 12.1.6 | All | All | All |
| Application | Symantec | Endpoint Protection | 12.1.6 | mp1 | All | All |
| Application | Symantec | Endpoint Protection | 12.1.6 | mp2 | All | All |
| Application | Symantec | Endpoint Protection | 12.1.6 | mp3 | All | All |
| Application | Symantec | Endpoint Protection | 12.1.6 | mp4 | All | All |
| Application | Symantec | Endpoint Protection | 12.1.6 | mp4 | All | All |
| Application | Symantec | Endpoint Protection | 12.1.6 | mp4 | All | All |
| Application | Symantec | Mail Security For Domino | All | All | All | All |
| Application | Symantec | Mail Security For Domino | All | All | All | All |
| Application | Symantec | Mail Security For Microsoft Exchange | 6.5.8 | All | All | All |
| Application | Symantec | Mail Security For Microsoft Exchange | 6.5.8 | All | All | All |
| Application | Symantec | Mail Security For Microsoft Exchange | All | All | All | All |
| Application | Symantec | Mail Security For Microsoft Exchange | All | All | All | All |
| Application | Symantec | Message Gateway | All | All | All | All |
| Application | Symantec | Message Gateway For Service Providers | 10.5 | All | All | All |
| Application | Symantec | Message Gateway For Service Providers | 10.6 | All | All | All |
| Application | Symantec | Message Gateway For Service Providers | 10.5 | All | All | All |
| Application | Symantec | Message Gateway For Service Providers | 10.6 | All | All | All |
| Application | Symantec | Ngc | All | All | All | All |
| Application | Symantec | Norton 360 | All | All | All | All |
| Application | Symantec | Norton 360 | All | All | All | All |
| Application | Symantec | Norton Antivirus | All | All | All | All |
| Application | Symantec | Norton Antivirus | All | All | All | All |
| Application | Symantec | Norton Bootable Removal Tool | All | All | All | All |
| Application | Symantec | Norton Internet Security | All | All | All | All |
| Application | Symantec | Norton Internet Security | All | All | All | All |
| Application | Symantec | Norton Power Eraser | All | All | All | All |
| Application | Symantec | Norton Security | All | All | All | All |
| Application | Symantec | Norton Security | All | All | All | All |
| Application | Symantec | Norton Security | All | All | All | All |
| Application | Symantec | Norton Security With Backup | All | All | All | All |

| | | | | | | |
|-------------|--------------------------|---|-------|-----|-----|-----|
| Application | Symantec | Norton Security With Backup | All | All | All | All |
| Application | Symantec | Protection Engine | 7.8.0 | All | All | All |
| Application | Symantec | Protection Engine | 7.8.0 | All | All | All |
| Application | Symantec | Protection Engine | All | All | All | All |
| Application | Symantec | Protection Engine | All | All | All | All |
| Application | Symantec | Protection For Sharepoint Servers | All | All | All | All |
| Application | Symantec | Protection For Sharepoint Servers | All | All | All | All |

References

Reference

[Symantec Endpoint Protection Flaws in Symantec Decomposer Engine Let Remote Users Execute Arbitrary Code - SecurityTracker](#)

[Symantec Antivirus - Missing Bounds Checks in dec2zip ALPkOldFormatDecompressor::UnShrink](#)

91435

[Norton Anti-Virus Flaws in Symantec Decomposer Engine Let Remote Users Execute Arbitrary Code - SecurityTracker](#)

[Security Advisories Relating to Symantec Products - Symantec Decomposer Engine Multiple Parsing Vulnerabilities - 2016-06-28T00:03:00 P](#)

[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](#).

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