



# CVE-2012-6277

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

## Summary

<b>CVE</b>	CVE-2012-6277
<b>State</b>	PUBLIC
<b>Assigner</b>	cert@cert.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-02-21 17:15:00 UTC
<b>Updated</b>	2020-03-04 20:18:00 UTC
<b>Description</b>	Multiple unspecified vulnerabilities in Autonomy KeyView IDOL before 10.16, as used in Symantec Mail Security for Microsc

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Hp</a>	<a href="#">Autonomy Keyview Idol</a>	All	All	All	All
Application	<a href="#">Hp</a>	<a href="#">Autonomy Keyview Idol</a>	All	All	All	All
Application	<a href="#">Ibm</a>	<a href="#">Domino</a>	All	All	All	All
Application	<a href="#">Ibm</a>	<a href="#">Notes</a>	All	All	All	All
Application	<a href="#">Symantec</a>	<a href="#">Data Loss Prevention Endpoint</a>	All	All	All	All
Application	<a href="#">Symantec</a>	<a href="#">Data Loss Prevention Endpoint</a>	All	All	All	All
Application	<a href="#">Symantec</a>	<a href="#">Data Loss Prevention Enforce/detection Servers</a>	All	All	All	All
Application	<a href="#">Symantec</a>	<a href="#">Data Loss Prevention Enforce/detection Servers</a>	All	All	All	All
Application	<a href="#">Symantec</a>	<a href="#">Data Loss Prevention Enforce/detection Servers</a>	All	All	All	All
Application	<a href="#">Symantec</a>	<a href="#">Data Loss Prevention Enforce/detection Servers</a>	All	All	All	All
Application	<a href="#">Symantec</a>	<a href="#">Data Loss Prevention Enforce/detection Servers</a>	All	All	All	All
Application	<a href="#">Symantec</a>	<a href="#">Data Loss Prevention Enforce/detection Servers</a>	All	All	All	All
Application	<a href="#">Symantec</a>	<a href="#">Mail Security</a>	6.5.7	All	All	All
Application	<a href="#">Symantec</a>	<a href="#">Mail Security</a>	6.5.7	All	All	All
Application	<a href="#">Symantec</a>	<a href="#">Mail Security</a>	All	All	All	All
Application	<a href="#">Symantec</a>	<a href="#">Mail Security</a>	All	All	All	All
Application	<a href="#">Symantec</a>	<a href="#">Messaging Gateway</a>	All	All	All	All

Application	Symantec	Messaging Gateway	All	All	All	All
-------------	----------	-------------------	-----	-----	-----	-----

## References

Reference
CVE-2012-6277
Autonomy Keyview IDOL Multiple Remote Code Execution Vulnerabilities
Vulnerability Note VU#849841 - Autonomy Keyview IDOL contains multiple vulnerabilities in file parsers
<a href="https://tools.cisco.com/security/center/viewAlert.x">tools.cisco.com/security/center/viewAlert.x</a>
Security Bulletin: Security vulnerabilities addressed in IBM Notes 9.0 (CVE-2011-3026, CVE-2012-6349, CVE-2012-6277) - IBM PSIRT Blog
V-118: IBM Lotus Domino Multiple Vulnerabilities   Department of Energy
Broadcom Support Portal
IBM Lotus Domino 8.5.x < 8.5.3 FP 4 Multiple Vulnerabilities   Tenable®
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](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://cve.mitre.org). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)