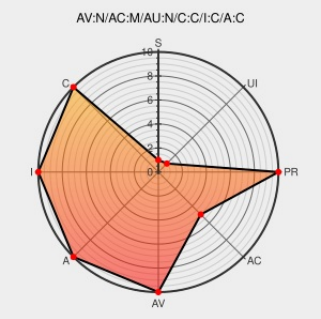
# CVE-2005-2619

Published on: 12/31/2005 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:27 PM UTC

## CVE-2005-2619

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Keyview Export Sdk from Autonomy contain the following vulnerability:

Directory traversal vulnerability in kvarcve.dll in Autonomy (formerly Verity) KeyView SDK before 9.2.0, as used in Lotus Notes 6.5.4 and 7.0, allows remote attackers to delete arbitrary files via a (1) ZIP, (2) UUE or (3) TAR archive that contains a .. (dot dot) in the filename, which is not properly handled when generating a preview.

CVE-2005-2619 has been assigned by cve@mitre.org to track the vulnerability

### CVSS2 Score: 9.3 - HIGH

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | MEDIUM | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| COMPLETE | COMPLETE | COMPLETE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| Secunia - Advisories - Verity KeyView SDK Multiple Vulnerabilities | Patch, Vendor Advisory, web.archive.org, text/html | SECUNIA 16100 |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | www.vupen.com, text/html | VUPEN ADV-2006-0500 |
| About Secunia Research \| Flexera | Vendor Advisory, secunia.com, Depreciated Link, text/html | MISC secunia.com/secunia_research/2005-66/advisory/ |
| IBM Lotus Notes File Attachment Handling Multiple Remote Vulnerabilities | cve.report (archive), text/html | BID 16576 |

| | | |
|---|---|---|
| No Description Provided | Patch<br>www.osvdb.org<br>Inactive Link Not Archived | OSVDB 23066 |
| IBM X-Force Exchange | exchange.xforce.ibmcloud.com<br>text/html | XF lotus-kvarcve-directory-traversal(24637) |
| SecurityFocus | www.securityfocus.com<br>text/html | BUGTRAQ 20060210 Secunia Research: Lotus Notes Multiple Archive Handling DirectoryTraversal |
| Secunia - Advisories - IBM Lotus Notes Multiple Vulnerabilities | Patch<br>Vendor Advisory<br>web.archive.org<br>text/html | SECUNIA 16280 |
| SecurityTracker.com Archives - IBM Lotus Domino/Notes Archive Processing Buffer Overflow and Directory Traversal Bugs Let Remote Users Execute Arbitrary Code and Delete Files | Patch<br>securitytracker.com<br>text/html | SECTRACK 1015657 |
| IBM Potential buffer overflow and directory traversal vulnerabilities in Lotus Notes file viewers - United States | Patch<br>web.archive.org<br>text/html<br>Inactive Link Not Archived | CONFIRM www-1.ibm.com/support/docview.wss?rs=475&uid=swg21229918 |
| About Secunia Research \| Flexera | Vendor Advisory<br>secunia.com<br>Depreciated Link<br>text/plain | MISC secunia.com/secunia_research/2005-30/advisory/ |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Autonomy | Keyview Export Sdk | All | All | All | All |
| Application | Autonomy | Keyview Export Sdk | All | All | All | All |
| Application | Autonomy | Keyview Filter Sdk | All | All | All | All |
| Application | Autonomy | Keyview Filter Sdk | All | All | All | All |
| Application | Autonomy | Keyview Viewer Sdk | All | All | All | All |
| Application | Autonomy | Keyview Viewer Sdk | All | All | All | All |
| Application | Ibm | Lotus Notes | 6.0.1 | All | All | All |
| Application | Ibm | Lotus Notes | 6.0.2 | All | All | All |
| Application | Ibm | Lotus Notes | 6.0.3 | All | All | All |
| Application | Ibm | Lotus Notes | 6.0.4 | All | All | All |
| Application | Ibm | Lotus Notes | 6.0.5 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Ibm | Lotus Notes | 6.5 | All | All | All |
| Application | Ibm | Lotus Notes | 6.5.1 | All | All | All |
| Application | Ibm | Lotus Notes | 6.5.2 | All | All | All |
| Application | Ibm | Lotus Notes | 6.5.3 | All | All | All |
| Application | Ibm | Lotus Notes | 6.5.4 | All | All | All |
| Application | Ibm | Lotus Notes | 7.0 | All | All | All |
| Application | Ibm | Lotus Notes | 6.0.1 | All | All | All |
| Application | Ibm | Lotus Notes | 6.0.2 | All | All | All |
| Application | Ibm | Lotus Notes | 6.0.3 | All | All | All |
| Application | Ibm | Lotus Notes | 6.0.4 | All | All | All |
| Application | Ibm | Lotus Notes | 6.0.5 | All | All | All |
| Application | Ibm | Lotus Notes | 6.5 | All | All | All |
| Application | Ibm | Lotus Notes | 6.5.1 | All | All | All |
| Application | Ibm | Lotus Notes | 6.5.2 | All | All | All |
| Application | Ibm | Lotus Notes | 6.5.3 | All | All | All |
| Application | Ibm | Lotus Notes | 6.5.4 | All | All | All |
| Application | Ibm | Lotus Notes | 7.0 | All | All | All |

cpe:2.3:a:autonomy:keyview_export_sdk:*:*:*:*:*:*:*:*:

cpe:2.3:a:autonomy:keyview_export_sdk:*:*:*:*:*:*:*:*:

cpe:2.3:a:autonomy:keyview_filter_sdk:*:*:*:*:*:*:*:*:

cpe:2.3:a:autonomy:keyview_filter_sdk:*:*:*:*:*:*:*:*:

cpe:2.3:a:autonomy:keyview_viewer_sdk:*:*:*:*:*:*:*:*:

cpe:2.3:a:autonomy:keyview_viewer_sdk:*:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_notes:6.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_notes:6.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_notes:6.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_notes:6.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_notes:6.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_notes:6.5:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_notes:6.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_notes:6.5.2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_notes:6.5.3:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_notes:6.5.4:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_notes:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_notes:6.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_notes:6.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_notes:6.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_notes:6.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_notes:6.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_notes:6.5:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_notes:6.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_notes:6.5.2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_notes:6.5.3:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_notes:6.5.4:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:lotus_notes:7.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→