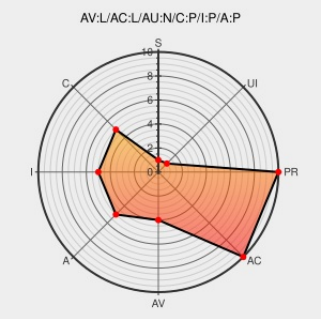
# CVE-2005-1961

Published on: 06/07/2005 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

## CVE-2005-1961

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




Certain versions of Consortium C-jdbc from Objectweb contain the following vulnerability:

Unknown vulnerability in ObjectWeb Consortium C-JDBC before 1.3.1 allows local users to bypass intended access restrictions and obtain the cache results from another user.

CVE-2005-1961 has been assigned by cve@mitre.org to track the vulnerability

## CVSS2 Score: 4.6 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| LOCAL | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | PARTIAL | PARTIAL |

## CVE References

| Description | Tags | Link |
|---|---|---|
| C-JDBC Exposure of Cached Results - Advisories - Secunia | Patch, Vendor Advisory, web.archive.org, text/html | SECUNIA 15627 |
| Clustered JDBC May Disclose a Target Users' Cached Results to Remote Users - SecurityTracker | Patch, Vendor Advisory, securitytracker.com, text/html | SECTRACK 1014118 |

There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Objectweb | Consortium C-jdbc | 1.0 | All | All | All |
| Application | Objectweb | Consortium C-jdbc | 1.0.1 | All | All | All |
| Application | Objectweb | Consortium C-jdbc | 1.0.2 | All | All | All |
| Application | Objectweb | Consortium C-jdbc | 1.0.3 | All | All | All |
| Application | Objectweb | Consortium C-jdbc | 1.0.4 | All | All | All |
| Application | Objectweb | Consortium C-jdbc | 1.1 | All | All | All |
| Application | Objectweb | Consortium C-jdbc | 1.2 | All | All | All |
| Application | Objectweb | Consortium C-jdbc | 1.2.1 | All | All | All |
| Application | Objectweb | Consortium C-jdbc | 1.3 | All | All | All |
| Application | Objectweb | Consortium C-jdbc | 1.0 | All | All | All |
| Application | Objectweb | Consortium C-jdbc | 1.0.1 | All | All | All |
| Application | Objectweb | Consortium C-jdbc | 1.0.2 | All | All | All |
| Application | Objectweb | Consortium C-jdbc | 1.0.3 | All | All | All |
| Application | Objectweb | Consortium C-jdbc | 1.0.4 | All | All | All |
| Application | Objectweb | Consortium C-jdbc | 1.1 | All | All | All |
| Application | Objectweb | Consortium C-jdbc | 1.2 | All | All | All |
| Application | Objectweb | Consortium C-jdbc | 1.2.1 | All | All | All |
| Application | Objectweb | Consortium C-jdbc | 1.3 | All | All | All |

cpe:2.3:a:objectweb:consortium_c-jdbc:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:objectweb:consortium_c-jdbc:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:objectweb:consortium_c-jdbc:1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:objectweb:consortium_c-jdbc:1.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:objectweb:consortium_c-jdbc:1.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:objectweb:consortium_c-jdbc:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:objectweb:consortium_c-jdbc:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:objectweb:consortium_c-jdbc:1.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:objectweb:consortium_c-jdbc:1.3:*:*:*:*:*:*:*:

cpe:2.3:a:objectweb:consortium_c-jdbc:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:objectweb:consortium_c-jdbc:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:objectweb:consortium_c-jdbc:1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:objectweb:consortium_c-jdbc:1.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:objectweb:consortium_c-jdbc:1.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:objectweb:consortium_c-jdbc:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:objectweb:consortium_c-jdbc:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:objectweb:consortium_c-jdbc:1.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:objectweb:consortium_c-jdbc:1.3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→