



# CVE-2005-0201

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

## Summary

<b>CVE</b>	CVE-2005-0201
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-06-29 04:00:00 UTC
<b>Updated</b>	2018-10-03 21:29:00 UTC
<b>Description</b>	D-BUS (dbus) before 0.22 does not properly restrict access to a socket, if the socket address is known, which allows local u

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	D-bus	D-bus	All	All	All	All

## References

Reference	Source	Link	Tags
Secunia - Advisories - Mandriva update for dbus	SECUNIA	<a href="https://secunia.com">secunia.com</a>	
Advisories - Mandriva	MANDRAKE	<a href="https://www.mandriva.com">www.mandriva.com</a>	Patch, Vendor
rhn.redhat.com   Red Hat Support	REDHAT	<a href="https://www.redhat.com">www.redhat.com</a>	Patch, Vendor
Secunia - Advisories - D-BUS Session Bus Hijack Vulnerability	SECUNIA	<a href="https://secunia.com">secunia.com</a>	
AusCERT - ESB-2005.0435 -- RHSA-2005:102-01 -- Low: dbus security update.	AUSCERT	<a href="https://www.auscert.org.au">www.auscert.org.au</a>	Vendor
USN-144-1: dbus vulnerability   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	
D-BUS Session Bus Local Privilege Escalation Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	
Repository / Oval Repository	OVAL	<a href="https://oval.cisecurity.org">oval.cisecurity.org</a>	
Secunia - Advisories - Ubuntu update for dbus	SECUNIA	<a href="https://secunia.com">secunia.com</a>	
Red Hat update for dbus - Advisories - Secunia	SECUNIA	<a href="https://secunia.com">secunia.com</a>	
SecurityTracker.com Archives - D-BUS Allows Local Users to Connect to the Session Bus	SECTRACK	<a href="https://securitytracker.com">securitytracker.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonic

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](#)**