



CVE-2011-2200

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2011-2200
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-06-22 22:55:04 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The _dbus_header_byteswap function in dbus-marshal-header.c in D-Bus (aka DBus) 1.2.x before 1.2.28, 1.4.x before 1.4.

Risk And Classification

Primary CVSS: v2.0 4.6 from nvd@nist.gov

AV:L/AC:L/Au:N/C:P/I:P/A:P

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:L/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	D-bus Project	D-bus	1.2.4.2	All	All	All

Application	D-bus Project	D-bus	1.2.4.4	All	All	All
Application	D-bus Project	D-bus	1.2.4.6	All	All	All
Application	Freedesktop	Dbus	1.2.1	All	All	All
Application	Freedesktop	Dbus	1.2.10	All	All	All
Application	Freedesktop	Dbus	1.2.12	All	All	All
Application	Freedesktop	Dbus	1.2.14	All	All	All
Application	Freedesktop	Dbus	1.2.16	All	All	All
Application	Freedesktop	Dbus	1.2.18	All	All	All
Application	Freedesktop	Dbus	1.2.2	All	All	All
Application	Freedesktop	Dbus	1.2.20	All	All	All
Application	Freedesktop	Dbus	1.2.22	All	All	All
Application	Freedesktop	Dbus	1.2.24	All	All	All
Application	Freedesktop	Dbus	1.2.26	All	All	All
Application	Freedesktop	Dbus	1.2.3	All	All	All
Application	Freedesktop	Dbus	1.2.4	All	All	All
Application	Freedesktop	Dbus	1.2.6	All	All	All
Application	Freedesktop	Dbus	1.2.8	All	All	All
Application	Freedesktop	Dbus	1.4.0	All	All	All
Application	Freedesktop	Dbus	1.4.1	All	All	All
Application	Freedesktop	Dbus	1.4.10	All	All	All
Application	Freedesktop	Dbus	1.4.4	All	All	All
Application	Freedesktop	Dbus	1.4.6	All	All	All
Application	Freedesktop	Dbus	1.4.8	All	All	All
Application	Freedesktop	Dbus	1.5.0	All	All	All
Application	Freedesktop	Dbus	1.5.2	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References						
Reference					Source	
D-Bus Message Byte Order Denial of Service Weakness - Secunia.com					af854a3a-2127-422f-b000-000000000000	
dbus/dbus - a lightweight ipc mechanism (mirrored from https://gitlab.freedesktop.org/dbus/dbus)					af854a3a-2127-422f-b000-000000000000	
oss-security - CVE Request -- dbus -- Local DoS via messages with non-native byte order					af854a3a-2127-422f-b000-000000000000	
Support					af854a3a-2127-422f-b000-000000000000	
oss-security - Bus#620028: Info received (CVE Request -- dbus -- Local DoS via messages with non-native byte order)					af854a3a-2127-422f-b000-000000000000	

oss-security - Bug#629938: info received (CVE Request -- dbus -- Local DoS via messages with non-native byte order)	af854a3a-2127-4221
#629938 - libdbus-1-3: [CVE-2011-2200] local DoS via messages with non-native byte order - Debian Bug report logs	af854a3a-2127-4221
oss-security - Re: CVE Request -- dbus -- Local DoS via messages with non-native byte order	af854a3a-2127-4221
dbus/dbus - a lightweight ipc mechanism (mirrored from https://gitlab.freedesktop.org/dbus/dbus)	af854a3a-2127-4221
Bug 712676 – CVE-2011-2200 dbus: Local DoS via messages with non-native byte order	af854a3a-2127-4221
D-Bus daemon big and little endian issue	af854a3a-2127-4221
Bug 38120 – byteswapping a message doesn't change the byte-order mark	af854a3a-2127-4221
IBM X-Force Exchange	af854a3a-2127-4221
Juniper Networks - 2015-10 Security Bulletin: CTPView: Multiple Vulnerabilities in CTPView	af854a3a-2127-4221
D-Bus daemon endianness issue	af854a3a-2127-4221
dbus/dbus - a lightweight ipc mechanism	af854a3a-2127-4221
dbus/dbus - a lightweight ipc mechanism	af854a3a-2127-4221
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#).

Free CVE JSON API [cve.report/api](#)

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