



CVE-2013-0238

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

Summary

CVE	CVE-2013-0238
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-02-13 01:55:00 UTC
Updated	2017-08-29 01:33:00 UTC
Description	The try_parse_v4_netmask function in hostmask.c in IRCD-Hybrid before 8.0.6 does not properly validate masks, which all

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	lrcd-hybrid	lrcd-hybrid	7.2.0	All	All	All
Application	lrcd-hybrid	lrcd-hybrid	7.2.1	All	All	All
Application	lrcd-hybrid	lrcd-hybrid	7.2.2	All	All	All
Application	lrcd-hybrid	lrcd-hybrid	7.2.3	All	All	All
Application	lrcd-hybrid	lrcd-hybrid	7.3.0	All	All	All
Application	lrcd-hybrid	lrcd-hybrid	7.3.0	rc1	All	All
Application	lrcd-hybrid	lrcd-hybrid	7.3.1	All	All	All
Application	lrcd-hybrid	lrcd-hybrid	8.0.0	All	All	All
Application	lrcd-hybrid	lrcd-hybrid	8.0.0	beta1	All	All
Application	lrcd-hybrid	lrcd-hybrid	8.0.0	beta2	All	All
Application	lrcd-hybrid	lrcd-hybrid	8.0.0	beta3	All	All
Application	lrcd-hybrid	lrcd-hybrid	8.0.0	rc1	All	All
Application	lrcd-hybrid	lrcd-hybrid	8.0.1	All	All	All
Application	lrcd-hybrid	lrcd-hybrid	8.0.2	All	All	All
Application	lrcd-hybrid	lrcd-hybrid	8.0.3	All	All	All
Application	lrcd-hybrid	lrcd-hybrid	8.0.4	All	All	All
Application	lrcd-hybrid	lrcd-hybrid	7.2.0	All	All	All

Application	lrcd-hybrid	lrcd-hybrid	7.2.1	All	All	All
Application	lrcd-hybrid	lrcd-hybrid	7.2.2	All	All	All
Application	lrcd-hybrid	lrcd-hybrid	7.2.3	All	All	All
Application	lrcd-hybrid	lrcd-hybrid	7.3.0	All	All	All
Application	lrcd-hybrid	lrcd-hybrid	7.3.0	rc1	All	All
Application	lrcd-hybrid	lrcd-hybrid	7.3.1	All	All	All
Application	lrcd-hybrid	lrcd-hybrid	8.0.0	All	All	All
Application	lrcd-hybrid	lrcd-hybrid	8.0.0	beta1	All	All
Application	lrcd-hybrid	lrcd-hybrid	8.0.0	beta2	All	All
Application	lrcd-hybrid	lrcd-hybrid	8.0.0	beta3	All	All
Application	lrcd-hybrid	lrcd-hybrid	8.0.0	rc1	All	All
Application	lrcd-hybrid	lrcd-hybrid	8.0.1	All	All	All
Application	lrcd-hybrid	lrcd-hybrid	8.0.2	All	All	All
Application	lrcd-hybrid	lrcd-hybrid	8.0.3	All	All	All
Application	lrcd-hybrid	lrcd-hybrid	8.0.4	All	All	All
Application	lrcd-hybrid	lrcd-hybrid	All	All	All	All

References

Reference

Source

Debian -- Security Information -- DSA-2618-1 lrcd-hybrid

DEBI

89623

OSVI

[svn] Diff of /lrcd-hybrid/trunk/src/hostmask.c

CONI

#699267 - lrcd-hybrid: CVE-2013-0238 Denial of service vulnerability in hostmask.c:try_parse_v4_netmask() - Debian Bug report logs

CONI

Support/Advisories/MGASA-2013-0055 - Mageia wiki

CONI

Support / Security / Advisories / / MDVSA-2013:093 | Mandriva

MANI

IBM X-Force Exchange

XF

IRCD-Hybrid 'try_parse_v4_netmask()' Denial of Service Vulnerability

BID

oss-security - lrcd-hybrid: Denial of service vulnerability in hostmask.c:try_parse_v4_netmask()

MLIS

Security Advisory SA51948 - IRCD-Hybrid "try_parse_v4_netmask()" Denial of Service Vulnerability - Secunia

SECU

Security Advisory SA52106 - Debian update for lrcd-hybrid - Secunia

SECU

lrcd-hybrid 8.0.5 - Denial of Service

EXPL

CVE Program record

CVE.

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](#)