



CVE-2011-5129

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

Summary

CVE	CVE-2011-5129
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-08-30 22:55:00 UTC
Updated	2013-02-14 04:47:00 UTC
Description	Heap-based buffer overflow in XChat 2.8.9 and earlier allows remote attackers to cause a denial of service (crash) and pos

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xchat	Xchat	1.2.1	All	All	All
Application	Xchat	Xchat	1.3.10	All	All	All
Application	Xchat	Xchat	1.3.11	All	All	All
Application	Xchat	Xchat	1.3.12	All	All	All
Application	Xchat	Xchat	1.3.13	All	All	All
Application	Xchat	Xchat	1.3.9	All	All	All
Application	Xchat	Xchat	1.4	All	All	All
Application	Xchat	Xchat	1.4.1	All	All	All
Application	Xchat	Xchat	1.4.2	All	All	All
Application	Xchat	Xchat	1.4.3	All	All	All
Application	Xchat	Xchat	1.5.6	All	All	All
Application	Xchat	Xchat	1.8.0	All	All	All
Application	Xchat	Xchat	1.8.1	All	All	All
Application	Xchat	Xchat	1.8.2	All	All	All
Application	Xchat	Xchat	1.8.3	All	All	All
Application	Xchat	Xchat	1.8.4	All	All	All
Application	Xchat	Xchat	1.8.5	All	All	All

Application	Xchat	Xchat	1.8.6	All	All	All
Application	Xchat	Xchat	1.8.7	All	All	All
Application	Xchat	Xchat	1.8.8	All	All	All
Application	Xchat	Xchat	1.8.9	All	All	All
Application	Xchat	Xchat	1.9.0	All	All	All
Application	Xchat	Xchat	1.9.1	All	All	All
Application	Xchat	Xchat	1.9.2	All	All	All
Application	Xchat	Xchat	1.9.3	All	All	All
Application	Xchat	Xchat	1.9.4	All	All	All
Application	Xchat	Xchat	1.9.5	All	All	All
Application	Xchat	Xchat	1.9.6	All	All	All
Application	Xchat	Xchat	1.9.7	All	All	All
Application	Xchat	Xchat	1.9.8	All	All	All
Application	Xchat	Xchat	1.9.9	All	All	All
Application	Xchat	Xchat	2.0.0	All	All	All
Application	Xchat	Xchat	2.0.1	All	All	All
Application	Xchat	Xchat	2.0.2	All	All	All
Application	Xchat	Xchat	2.0.3	All	All	All
Application	Xchat	Xchat	2.0.4	All	All	All
Application	Xchat	Xchat	2.0.5	All	All	All
Application	Xchat	Xchat	2.0.6	All	All	All
Application	Xchat	Xchat	2.0.7	All	All	All
Application	Xchat	Xchat	2.0.8	All	All	All
Application	Xchat	Xchat	2.6.7	All	All	All
Application	Xchat	Xchat	2.8.0	All	All	All
Application	Xchat	Xchat	2.8.1	All	All	All
Application	Xchat	Xchat	2.8.3	All	All	All
Application	Xchat	Xchat	2.8.3	c	All	All
Application	Xchat	Xchat	2.8.3	e	All	All
Application	Xchat	Xchat	2.8.4	All	All	All
Application	Xchat	Xchat	2.8.5	b	All	All
Application	Xchat	Xchat	2.8.5	e	All	All
Application	Xchat	Xchat	2.8.6	All	All	All
Application	Xchat	Xchat	2.8.7	a	All	All
Application	Xchat	Xchat	2.8.7	b	All	All

Application	Xchat	Xchat	2.8.7	c	All	All
Application	Xchat	Xchat	2.8.7	d	All	All
Application	Xchat	Xchat	2.8.7	e	All	All
Application	Xchat	Xchat	2.8.7	f	All	All
Application	Xchat	Xchat	2.8.7b	All	All	All
Application	Xchat	Xchat	2.8.8	All	All	All
Application	Xchat	Xchat	1.2.1	All	All	All
Application	Xchat	Xchat	1.3.10	All	All	All
Application	Xchat	Xchat	1.3.11	All	All	All
Application	Xchat	Xchat	1.3.12	All	All	All
Application	Xchat	Xchat	1.3.13	All	All	All
Application	Xchat	Xchat	1.3.9	All	All	All
Application	Xchat	Xchat	1.4	All	All	All
Application	Xchat	Xchat	1.4.1	All	All	All
Application	Xchat	Xchat	1.4.2	All	All	All
Application	Xchat	Xchat	1.4.3	All	All	All
Application	Xchat	Xchat	1.5.6	All	All	All
Application	Xchat	Xchat	1.8.0	All	All	All
Application	Xchat	Xchat	1.8.1	All	All	All
Application	Xchat	Xchat	1.8.2	All	All	All
Application	Xchat	Xchat	1.8.3	All	All	All
Application	Xchat	Xchat	1.8.4	All	All	All
Application	Xchat	Xchat	1.8.5	All	All	All
Application	Xchat	Xchat	1.8.6	All	All	All
Application	Xchat	Xchat	1.8.7	All	All	All
Application	Xchat	Xchat	1.8.8	All	All	All
Application	Xchat	Xchat	1.8.9	All	All	All
Application	Xchat	Xchat	1.9.0	All	All	All
Application	Xchat	Xchat	1.9.1	All	All	All
Application	Xchat	Xchat	1.9.2	All	All	All
Application	Xchat	Xchat	1.9.3	All	All	All
Application	Xchat	Xchat	1.9.4	All	All	All
Application	Xchat	Xchat	1.9.5	All	All	All
Application	Xchat	Xchat	1.9.6	All	All	All
Application	Xchat	Xchat	1.9.7	All	All	All
Application	Xchat	Xchat	1.9.8	All	All	All

Application	Xchat	Xchat	1.9.8	All	All	All
Application	Xchat	Xchat	1.9.9	All	All	All
Application	Xchat	Xchat	2.0.0	All	All	All
Application	Xchat	Xchat	2.0.1	All	All	All
Application	Xchat	Xchat	2.0.2	All	All	All
Application	Xchat	Xchat	2.0.3	All	All	All
Application	Xchat	Xchat	2.0.4	All	All	All
Application	Xchat	Xchat	2.0.5	All	All	All
Application	Xchat	Xchat	2.0.6	All	All	All
Application	Xchat	Xchat	2.0.7	All	All	All
Application	Xchat	Xchat	2.0.8	All	All	All
Application	Xchat	Xchat	2.6.7	All	All	All
Application	Xchat	Xchat	2.8.0	All	All	All
Application	Xchat	Xchat	2.8.1	All	All	All
Application	Xchat	Xchat	2.8.3	All	All	All
Application	Xchat	Xchat	2.8.3	c	All	All
Application	Xchat	Xchat	2.8.3	e	All	All
Application	Xchat	Xchat	2.8.4	All	All	All
Application	Xchat	Xchat	2.8.5	b	All	All
Application	Xchat	Xchat	2.8.5	e	All	All
Application	Xchat	Xchat	2.8.6	All	All	All
Application	Xchat	Xchat	2.8.7	a	All	All
Application	Xchat	Xchat	2.8.7	b	All	All
Application	Xchat	Xchat	2.8.7	c	All	All
Application	Xchat	Xchat	2.8.7	d	All	All
Application	Xchat	Xchat	2.8.7	e	All	All
Application	Xchat	Xchat	2.8.7	f	All	All
Application	Xchat	Xchat	2.8.7b	All	All	All
Application	Xchat	Xchat	2.8.8	All	All	All
Application	Xchat	Xchat	All	All	All	All

References

Reference	Source	Link	Tags
XChat 2.8.9 Heap Overflow ≈ Packet Storm	MISC	packetstormsecurity.org	Exploit
77629	OSVDB	www.osvdb.org	
XChat Heap Overflow Lets Remote Users Deny Service - SecurityTracker	SECTRACK	www.securitytracker.com	

XChat Remote Denial of Service Vulnerability	BID	www.securityfocus.com	Exploit
XChat Heap Overflow DoS	EXPLOIT-DB	www.exploit-db.com	Exploit
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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