



CVE-2008-3188

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

Summary

CVE	CVE-2008-3188
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-07-22 16:41:00 UTC
Updated	2021-03-30 14:07:00 UTC
Description	libxcrypt in SUSE openSUSE 11.0 uses the DES algorithm when the configuration specifies the MD5 algorithm, which makes it vulnerable to a brute force attack.

Risk And Classification

Problem Types: CWE-326

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Opensuse	Libxcrypt	All	All	All	All
Application	Opensuse	Libxcrypt	All	All	All	All
Operating System	Opensuse	Opensuse	11.0	All	All	All
Operating System	Opensuse	Opensuse	11.0	All	All	All
Operating System	Opensuse	Opensuse	11.0	All	All	All

References

Reference	Source
[security-announce] SUSE Security Announcement: libxcrypt (SUSE-SA:2008:016)	SUSE
openSUSE libxcrypt MD5 Password Hash Configuration Weakness - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
openSUSE 'libxcrypt' Insecure Password Hash Weakness	BID
[security-announce] SUSE Security Summary Report: SUSE-SR:2008:016	SUSE
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
IBM X-Force Exchange	XF
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](#)