CVE-2011-2709

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

Summary

CVE	CVE-2011-2709
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-06-21 15:55:00 UTC
Updated	2013-03-02 04:33:00 UTC
Description	libgssapi and libgssglue before 0.4 do not properly check privileges, which allows local users to load untrusted configuration

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Umich	Libgssapi	0.1	All	All	All
Application	Umich	Libgssapi	0.2	All	All	All
Application	Umich	Libgssapi	All	All	All	All
Application	Umich	Libgssapi	0.1	All	All	All
Application	Umich	Libgssapi	0.2	All	All	All
Application	Umich	Libgssglue	0.1	All	All	All
Application	Umich	Libgssglue	0.2	All	All	All
Application	Umich	Libgssglue	All	All	All	All
Application	Umich	Libgssglue	0.1	All	All	All
Application	Umich	Libgssglue	0.2	All	All	All

References

Reference
oss-security - Re: CVE Request -- libgssapi, libgssglue -- Ability to load untrusted configuration file, when loading GSS mechanisms and their
SUSE alert SUSE-SU-2011:0696-1 (libgssglue) [LWN.net]
[SECURITY] Fedora 17 Update: libgssglue-0.4-0.fc17
www.citi.umich.edu/projects/nfsv4/linux/libgssglue/libgssglue-0.4.tar.gz

[SECURITY] Fedora 16 Update: libgssglue-0.4-0.fc16
Access Denied
Security Advisory SA50973 - Ubuntu update for libgssglue - Secunia
SUSE update for libgssglue - Secunia.com
oss-security - CVE Request -- libgssapi, libgssglue -- Ability to load untrusted configuration file, when loading GSS mechanisms and their defir
Security Alerts - Secunia
oss-security - Re: CVE Request -- libgssapi, libgssglue -- Ability to load untrusted configuration file, when loading GSS mechanisms and their
libgssglue 'GSSAPI_MECH_CONF' Environment Variable Local Privilege Escalation Vulnerability
CVE Program record
NVD vulnerability detail

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 registred 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**