



# CVE-2011-2914

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

## Summary

|                        |                                                                                                                          |
|------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2011-2914                                                                                                            |
| <b>State</b>           | PUBLIC                                                                                                                   |
| <b>Assigner</b>        | secalert@redhat.com                                                                                                      |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                             |
| <b>Published</b>       | 2012-06-07 19:55:00 UTC                                                                                                  |
| <b>Updated</b>         | 2023-02-13 00:19:00 UTC                                                                                                  |
| <b>Description</b>     | Off-by-one error in the CSoundFile::ReadDSM function in src/load_dms.cpp in libmodplug before 0.8.8.4 allows remote atta |

## Risk And Classification

### Problem Types: CWE-189

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                               | Product                    | Version | Update | Edition | Language |
|-------------|--------------------------------------|----------------------------|---------|--------|---------|----------|
| Application | <a href="#">Konstanty Bialkowski</a> | <a href="#">Libmodplug</a> | 0.8     | All    | All     | All      |
| Application | <a href="#">Konstanty Bialkowski</a> | <a href="#">Libmodplug</a> | 0.8.4   | All    | All     | All      |
| Application | <a href="#">Konstanty Bialkowski</a> | <a href="#">Libmodplug</a> | 0.8.5   | All    | All     | All      |
| Application | <a href="#">Konstanty Bialkowski</a> | <a href="#">Libmodplug</a> | 0.8.6   | All    | All     | All      |
| Application | <a href="#">Konstanty Bialkowski</a> | <a href="#">Libmodplug</a> | 0.8.7   | All    | All     | All      |
| Application | <a href="#">Konstanty Bialkowski</a> | <a href="#">Libmodplug</a> | 0.8.8   | All    | All     | All      |
| Application | <a href="#">Konstanty Bialkowski</a> | <a href="#">Libmodplug</a> | 0.8.8.1 | All    | All     | All      |
| Application | <a href="#">Konstanty Bialkowski</a> | <a href="#">Libmodplug</a> | 0.8.8.2 | All    | All     | All      |
| Application | <a href="#">Konstanty Bialkowski</a> | <a href="#">Libmodplug</a> | All     | All    | All     | All      |
| Application | <a href="#">Konstanty Bialkowski</a> | <a href="#">Libmodplug</a> | 0.8     | All    | All     | All      |
| Application | <a href="#">Konstanty Bialkowski</a> | <a href="#">Libmodplug</a> | 0.8.4   | All    | All     | All      |
| Application | <a href="#">Konstanty Bialkowski</a> | <a href="#">Libmodplug</a> | 0.8.5   | All    | All     | All      |
| Application | <a href="#">Konstanty Bialkowski</a> | <a href="#">Libmodplug</a> | 0.8.6   | All    | All     | All      |
| Application | <a href="#">Konstanty Bialkowski</a> | <a href="#">Libmodplug</a> | 0.8.7   | All    | All     | All      |
| Application | <a href="#">Konstanty Bialkowski</a> | <a href="#">Libmodplug</a> | 0.8.8   | All    | All     | All      |
| Application | <a href="#">Konstanty Bialkowski</a> | <a href="#">Libmodplug</a> | 0.8.8.1 | All    | All     | All      |
| Application | <a href="#">Konstanty Bialkowski</a> | <a href="#">Libmodplug</a> | 0.8.8.2 | All    | All     | All      |

## References

| Reference                                                                                   | Source  | Link                                                                                    |
|---------------------------------------------------------------------------------------------|---------|-----------------------------------------------------------------------------------------|
| Security Advisory SA48439 - Gentoo update for audacious-plugins - Secunia                   | SECUNIA | <a href="https://secunia.com">secunia.com</a>                                           |
| Gentoo Linux Documentation -- ModPlug: User-assisted execution of arbitrary code            | GENTOO  | <a href="http://www.gentoo.org">www.gentoo.org</a>                                      |
| access.redhat.com                                                                           | REDHAT  | <a href="https://rhn.redhat.com">rhn.redhat.com</a>                                     |
| jira.atheme.org/browse/AUDPLUG-394                                                          | CONFIRM | <a href="https://jira.atheme.org">jira.atheme.org</a>                                   |
| Security Advisory SA46793 - Ubuntu update for libmodplug - Secunia                          | SECUNIA | <a href="https://secunia.com">secunia.com</a>                                           |
| oss-security - CVE request: libmodplug: multiple vulnerabilities reported in <= 0.8.8.3     | MLIST   | <a href="http://www.openwall.com">www.openwall.com</a>                                  |
| USN-1255-1: libmodplug vulnerabilities   Ubuntu                                             | UBUNTU  | <a href="https://ubuntu.com">ubuntu.com</a>                                             |
| Gentoo Linux Documentation -- Audacious Plugins: User-assisted execution of arbitrary code  | GENTOO  | <a href="http://www.gentoo.org">www.gentoo.org</a>                                      |
| Red Hat update for gstreamer-plugins - Secunia.com                                          | SECUNIA | <a href="https://secunia.com">secunia.com</a>                                           |
| Audacious Plugins libmodplug Multiple Vulnerabilities - Secunia.com                         | SECUNIA | <a href="https://secunia.com">secunia.com</a>                                           |
| 74211                                                                                       | OSVDB   | <a href="http://www.osvdb.org">www.osvdb.org</a>                                        |
| oss-security - Re: CVE request: libmodplug: multiple vulnerabilities reported in <= 0.8.8.3 | MLIST   | <a href="http://www.openwall.com">www.openwall.com</a>                                  |
| Security Advisory SA48058 - Debian update for libmodplug - Secunia                          | SECUNIA | <a href="https://secunia.com">secunia.com</a>                                           |
| libmodplug Multiple Buffer Overflow and Off-By-One Vulnerabilities                          | BID     | <a href="http://www.securityfocus.com">www.securityfocus.com</a>                        |
| Security Advisory SA46043 - Fedora update for audacious-plugins - Secunia                   | SECUNIA | <a href="https://secunia.com">secunia.com</a>                                           |
| Debian -- Security Information -- DSA-2415-1 libmodplug                                     | DEBIAN  | <a href="http://www.debian.org">www.debian.org</a>                                      |
| Security Advisory SA45658 - Fedora update for libmodplug - Secunia                          | SECUNIA | <a href="https://secunia.com">secunia.com</a>                                           |
| IBM X-Force Exchange                                                                        | XF      | <a href="https://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>         |
| ModPlug for XMMS - Browse /libmodplug/0.8.8.4 at SourceForge.net                            | CONFIRM | <a href="https://sourceforge.net">sourceforge.net</a>                                   |
| SUSE update for libmodplug - Secunia.com                                                    | SECUNIA | <a href="https://secunia.com">secunia.com</a>                                           |
| ModPlug for XMMS / Git tools                                                                | CONFIRM | <a href="https://modplug-xmms.git.sourceforge.net">modplug-xmms.git.sourceforge.net</a> |
| [SECURITY] Fedora 14 Update: libmodplug-0.8.8.4-1.fc14                                      | FEDORA  | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>                   |
| [SECURITY] Fedora 14 Update: audacious-plugins-2.4.5-4.fc14                                 | FEDORA  | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>                   |
| Security Advisory SA48434 - Gentoo update for libmodplug - Secunia                          | SECUNIA | <a href="https://secunia.com">secunia.com</a>                                           |
| [security-announce] openSUSE-SU-2011:0943-1: important: libmodplug: Fixe                    | SUSE    | <a href="https://lists.opensuse.org">lists.opensuse.org</a>                             |
| libmodplug Multiple Vulnerabilities - Secunia.com                                           | SECUNIA | <a href="https://secunia.com">secunia.com</a>                                           |
| ModPlug for XMMS / Git tools                                                                | MISC    | <a href="https://modplug-xmms.git.sourceforge.net">modplug-xmms.git.sourceforge.net</a> |
| CVE Program record                                                                          | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>                                            |
| NVD vulnerability detail                                                                    | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                                         |

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](#)