

[NEWS] LimeWire Gnutella Client Directory Traversal and File Disclosure

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0078.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/17/05

To: list@securiteam.com

Date: 17 Mar 2005 11:37:28 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

LimeWire Gnutella Client Directory Traversal and File Disclosure

SUMMARY

" <<http://www.limewire.com/>> LimeWire is a file sharing program running on the Gnutella Network. It is open standard software running on an open protocol, free for the public to use. LimeWire allows you to share any file such as mp3s, avis, jpgs, tiffs, etc. Limewire is written in Java, and will run on Windows, Macintosh, Linux, Sun, and other computing platforms."

Recent versions of the LimeWire client contain vulnerabilities that allow a remote user to access many or all files on a users machine.

DETAILS

Vulnerable Systems:

* LimeWire versions 4.1.2 up to 4.5.6 are vulnerable to File Disclosure

* LimeWire versions 3.9.6 up to 4.6.0 are vulnerable to Directory Traversal

Immune Systems:

* LimeWire version 4.6.0 (File Disclosure)

Securiteam: [NEWS] LimeWire Gnutella Client Directory Traversal and File Disclosure

* LimeWire version 4.8.0 (Directory Traversal)

File Disclosure Vulnerability (Inappropriate handling of "resource get" requests):

A remote attacker can request and read any file on a host running an affected version of LimeWire. Gnutella "push style" requests is also vulnerable under most conditions, and therefore a local firewall does not prevent the attack. The files accessible to a remote attacker include all of the user's private, local files, and any file on the machine if the user has administrator privileges, a common scenario in Windows. The handling of "resource get" requests is the immediate cause of the problem. A request of the form `"/gnutella/res/[filename]"` returns the named file. For example, one can telnet to a LimeWire client using the default LimeWire port and type the following text:

```
GET /gnutella/res/C:\Windows\win.ini HTTP/1.1
User-Agent: I-AM-AN-ATTACKER/1.0
Host: 0.0.0.0:0
Accept: */*
Connection: Keep-Alive
```

The result is that the LimeWire client reads the file `"C:\Windows\win.ini"` and sends it over the network. Similarly, the attacker may request `"/gnutella/res//etc/passwd"` on Linux or UNIX-based machines. This attack has been tested and confirmed on Linux and Windows 2000 platforms.

Workaround:

This problem has been fixed in the recently released LimeWire versions 4.6.0 and later, which were released promptly by Lime Wire LLC after notification of the vulnerability.

Directory Traversal Vulnerability (Inappropriate handling of "magnet" requests):

A remote attacker can request and read any file on a host running an affected version of LimeWire. The attacker need only be able to connect to the LimeWire client "magnet" TCP port (default port, or a port chosen from a modest range if default is not available). Gnutella "push style" requests are not vulnerable, so a firewall that blocks access to the magnet port blocks the attack. The files accessible to a remote attacker include all of the user's private, local files, and any file on the machine if the user has administrator privileges.

The handling of "magnet" requests is the immediate cause of the problem. A request of the form `"/magnet10/[rel-filename]"` returns the named file, relative to the "root" subdirectory of the LimeWire installation, regardless of if it is in the "root" directory, or indeed even part of the LimeWire package. For example, one can telnet to a LimeWire client and issue an HTTP request

```
"GET /magnet10/../../../../Windows/Win.ini?Simple-test"
```

This example assumes that LimeWire is installed in its default installation directory. The result is that the LimeWire client reads the

Securiteam: [NEWS] LimeWire Gnutella Client Directory Traversal and File Disclosure

file "C:\Windows\win.ini" and sends it over the network. Similarly attacks work on Linux or UNIX-based machines. The attack has been tested and confirmed on Linux and Windows 2000 platforms, using several versions of LimeWire.

Workaround:

This problem has been fixed in the recently released LimeWire versions 4.8.0 and later, which were released promptly by Lime Wire LLC notification of the vulnerability.

ADDITIONAL INFORMATION

The information has been provided by <mailto:kwalsh@cs.cornell.edu> Kevin Walsh.

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind. In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.