

[NEWS] PeerCast Format String

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-05/0163.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 05/31/05

To: list@securiteam.com

Date: 31 May 2005 18:14:45 +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>

PeerCast Format String

SUMMARY

<<http://www.peercast.org/>> PeerCast is a popular p2p streaming media server (similar to shoutcast) – "PeerCast is a new, free way to listen to radio and watch video on the Internet. It uses P2P technology to let anyone become a broadcaster without the costs of traditional streaming. This means you get to hear and watch stations not normally found on commercially funded sites."

PeerCast is vulnerable to format string vulnerability, attackers exploiting this vulnerability can cause the server to execute arbitrary code.

DETAILS

Vulnerable Systems:

* Peercast versions 0.1211 and prior

Immune Systems:

* PeerCast version 0.1212

There is a format string issue in PeerCast that allows an attacker to execute arbitrary code on the remote target with the privileges of the

Securiteam: [NEWS] PeerCast Format String

user running PeerCast or crash the server.

Below is an example of how this vulnerability can be exploited to crash a vulnerable server:

<http://localhost:7144/html/en/index.htm%n>

The problem occurs because of the way some error messages are handled. For example in the above example the PeerCast server receives a malformed request, so the error routine printed the URL, but the error print routine (because it was a printf type function call) then tries to parse the malicious URL.

Patch Availability:

An immune version was release shortly after vendor notification and is available from:

<<http://www.peercast.org/forum/viewtopic.php?p=11596>>
<http://www.peercast.org/forum/viewtopic.php?p=11596>

ADDITIONAL INFORMATION

The information has been provided by James Bercegay.

The original article can be found at:

<http://www.gulftech.org/?node=research&article_id=00077-05282005>
http://www.gulftech.org/?node=research&article_id=00077-05282005

=====

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.