

[NEWS] Liferay Cross Site Scripting Flaw

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-05/0080.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 05/24/04

To: list@securiteam.com

Date: 24 May 2004 18:57:16 +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>

Liferay Cross Site Scripting Flaw

SUMMARY

<<http://www.liferay.com/products/index.jsp>> Liferay Enterprise Portal "was designed to provide organizations with a single sign-on web interface for email, document management, message board, and other useful communication tools. Multiple authentication schemes (LDAP or SQL) are pooled together so users don't have to remember a different login and password for every section of the portal".

Liferay Enterprise Portal is prone to a cross-site scripting in many places where user input is received.

DETAILS

Vulnerable Systems:

* Liferay Enterprise Portal version 2.1.1 and prior

Almost all fields that take input from the user's browser are prone to XSS attacks. Inadequate filtering makes it easy for an attacker to cause the victim's browser to execute script code. For example, the following code can be somewhat problematic when embedded in HTML:

```
<scr!pt>history.go(-1)</scr!pt>
```

Securiteam: [NEWS] Liferay Cross Site Scripting Flaw

ADDITIONAL INFORMATION

The information has been provided by <mailto:giris@deshaw.com> Giri, Sandeep.

=====

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.