

[NEWS] Lycos Free Email Cross-Site Scripting Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0110.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 12/28/04

To: list@securiteam.com

Date: 28 Dec 2004 09:49:25 +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>

Lycos Free Email Cross-Site Scripting Vulnerability

SUMMARY

Lycos's Free Email service "allows users to have their own web based email account very much like Hotmail". A cross site scripting vulnerability in Lycos's Free Email service allows an attacker to steal a user's cookie allowing him full access to his Lycos email account. Further, due to a flaw in the way Lycos handles cookies, even if the user being attacked changes his password, the attacker can still gain access to his account as the cookie will remain valid.

DETAILS

Proof of Concept:

The following URL will trigger the vulnerability in Lycos:

http://ldbreg.lycos.com/cgi-bin/mayaRegister?m_NP=%22%3E%3C

[script%3Ealert\(document.cookie\)%3C/script%3EEUSA_LycosMail_Plus&m_RC=32&m_PR=27&](http://ldbreg.lycos.com/cgi-bin/mayaRegister?m_NP=%22%3E%3Cscript%3Ealert(document.cookie)%3C/script%3EEUSA_LycosMail_Plus&m_RC=32&m_PR=27&)

ADDITIONAL INFORMATION

The information has been provided by <mailto:goldshlager@gmail.com> Nir Goldshlager.

Securiteam: [NEWS] Lycos Free Email Cross-Site Scripting Vulnerability

=====

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.