

[UNIX] Lynx Command Execution

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0048.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/14/05

To: list@securiteam.com

Date: 14 Nov 2005 16:18:20 +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>

Lynx Command Execution

SUMMARY

" <<http://lynx.browser.org/>> Lynx is a text browser for the World Wide Web."

Improper configuration of the CGI execution by Lynx allows attackers to cause the program to execute arbitrary programs.

DETAILS

Vulnerable Systems:

* Lynx, version 2.8.5

Immune Systems:

* Lynx version 2.8.6dev.15

The problem specifically exists within the feature to execute local cgi-bin programs via the "lynxcgi:" URI handler. The handler is generally intended to be restricted to a specific directory or program(s). However, due to a configuration error on multiple platforms, the default settings allow for arbitrary websites to specify commands to run as the user running Lynx.

Securiteam: [UNIX] Lynx Command Execution

Successful exploitation of the described vulnerability allows remote attackers to execute arbitrary commands with the privileges of the underlying user. Exploitation requires that an attacker convince a target user to follow a malicious link from within a vulnerable version of Lynx. The "lynxexec" and "lynxprog" URI handlers can also be used to trigger the issue. However, they are rarely compiled into the Lynx binary.

Workaround:

Disable "lynxcgi" links by specifying the following directive in lynx.cfg:

```
TRUSTED_LYNXCGI:none
```

Vendor Status:

Development version 2.8.6dev.15 has been released to address this issue and is available from the following URLs:

<<http://lynx.isc.org/current/lynx2.8.6dev.15.tar.Z>>
<http://lynx.isc.org/current/lynx2.8.6dev.15.tar.Z>,
<<http://lynx.isc.org/current/lynx2.8.6dev.15.tar.bz2>>
<http://lynx.isc.org/current/lynx2.8.6dev.15.tar.bz2>,
<<http://lynx.isc.org/current/lynx2.8.6dev.15.tar.gz>>
<http://lynx.isc.org/current/lynx2.8.6dev.15.tar.gz>,
<<http://lynx.isc.org/current/lynx2.8.6dev.15.zip>>
<http://lynx.isc.org/current/lynx2.8.6dev.15.zip>

Alternately, an incremental patch is available at:

<<http://lynx.isc.org/current/2.8.6dev.15.patch.gz>>
<http://lynx.isc.org/current/2.8.6dev.15.patch.gz>

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2929>>
CVE-2005-2929

Disclosure Timeline:

10/27/2005 – Initial vendor notification
10/28/2005 – Initial vendor response
11/11/2005 – Public disclosure

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:idlabs-advisories@lists.iddefense.com>> iDEFENSE Labs.

The original article can be found at:

<<http://www.iddefense.com/application/poi/display?id=338&type=vulnerabilities&flashstatus=true>>
<http://www.iddefense.com/application/poi/display?id=338&type=vulnerabilities>

=====

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

Securiteam: [UNIX] Lynx Command Execution

=====
=====

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.