

[UNIX] Lynx CRLF Injection

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0056.html>

From: support@securiteam.com

Date: 08/19/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 19 Aug 2002 10:51:26 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Lynx CRLF Injection

SUMMARY

Lynx is a fully featured World Wide Web (WWW) client for users running cursor-addressable, character-cell display devices such as vt100 terminals, vt100 emulators running on Windows 95/NT or Macintoshes, or any other character-cell display. By giving Lynx a URL with some special characters on the command line, it can be caused to include bogus headers in its HTTP query. This will allow you to make scripts that use Lynx for downloading files from wrong site on a web server with multiple virtual hosts.

DETAILS

Vulnerable systems:

- * Lynx versions 2.8.4rel.1, 2.8.5dev.8, 2.8.3rel.1, 2.8.2rel.1, possibly others

Immune systems:

- * Lynx version 2.8.4rel.1 with all patches applied

Technical details:

When a URL is given on the command line or in the WWW_HOME environment variable, Lynx does not remove or encode dangerous characters such as space, tab, CR and LF before constructing HTTP queries. This means that an

Securiteam: [UNIX] Lynx CRLF Injection

attacker can construct a URL that will send arbitrary faked HTTP headers, by adding space + "HTTP/1.0" + CRLF + some headers + CRLF + CRLF after the normal URL. Lynx's own HTTP headers are sent after the faked headers, but the web server ignores them, as our CRLF + CRLF pair above indicates the end of the headers.

This may cause some security problems. One scenario is when a program starts Lynx, and the host part of the URL is supplied by the program and the path by its user (something like "lynx [http://www.site3.st/\\$path](http://www.site3.st/$path)", where the value of \$path is defined by the user). An attacker can make such a program access some other web site than www.site3.st, if it's a virtual host on the same machine as www.site3.st, by adding a "Host:" header as described above.

Relative links do not work in web pages that are fetched this way. If there is a relative link like [Sunnan](#) and the user follows it, Lynx gets confused.

To get more information about this type of hole, read my paper "CRLF Injection", this is available at <http://www.securiteam.com/securityreviews/5WP022K75O.html>> CRLF Injection

Perl exploit:

```
#!/usr/bin/perl --
# Ulf Harnhammar 2002
# example: ./exploit www.site1.st www.site2.st
# will show www.site2.st
```

```
die "$0 hostone hosttwo\n" if @ARGV != 2;
```

```
exec('lynx "'
      "http://\$ARGV\[0\]/ HTTP/1.0\012".
      "Host: $ARGV[1]\012\012".
      "");
```

Bash command line exploit:

(This exploit assumes that www.site1.st and www.site2.st are virtual hosts on the same machine. Lynx will show www.site2.st.)

```
[ulf@metaur ulf]$ lynx "http://www.site1.st/ HTTP/1.0
Host: www.site2.st
```

"

Vendor status:

The vendor was contacted on 13 August. Their patch was released and announced on the Lynx-Dev list on the 18th.

Patch:

A patch can be downloaded from:

```
<ftp://lynx.isc.org/lynx2.8.4/patches/lynx2.8.4rel.1c.patch>
```

Securiteam: [UNIX] Lynx CRLF Injection

<ftp://lynx.isc.org/lynx2.8.4/patches/lynx2.8.4rel.1c.patch>

ADDITIONAL INFORMATION

The information has been provided by <mailto:ulfh@update.uu.se> Ulf Harnhammar.

=====

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.

-
- *Previous message:* support@securiteam.com: "[UNIX] FUDforum file access and SQL Injection"
 - *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)