

[UNIX] ListProc Mailing List ULISTPROC_UMASK Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-05/0011.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 05/09/03

To: list@securiteam.com

Date: 9 May 2003 09:45:16 +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

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

ListProc Mailing List ULISTPROC_UMASK Overflow

SUMMARY

<<http://sourceforge.net/projects/listproc/>> ListProc is a UNIX based automated information distribution and retrieval system for electronic mailing lists and file archives. ListProc is intended to be easy to maintain, support, and use. A local buffer overflow in the product allows local attackers to gain elevated privileges.

DETAILS

Vulnerable systems:

* ListProc version 8.2.09 and prior

In the middle of July last year, The Corporation for Research and Educational Networking (CREN) was notified of a local buffer overflow in the program known as Catmail. Catmail is a helper application for the mailing list server ListProc. ListProc is "the UNIX Mailing List Manager of choice" for a number of companies.

Securiteam: [UNIX] ListProc Mailing List ULISTPROC_UMASK Overflow

On January 7, 2003 CREN has effectively ceased all operations including work with ListProc with the following statement: "We recommend that the Corporation for Research and Educational Networking (CREN) be dissolved effective as soon as appropriate. The effective date of dissolution will likely be in the first quarter of 2003. CREN Operations will cease effective as soon as appropriate."

Prior to the company stopping operations SecNetOps was in contact with their development staff long enough to see that a fix was created for the above-mentioned issue. Unfortunately, at the time their staff was not on hand to thoroughly test the fix. SecNetOps did not have the facilities to compile the new version of Catmail in efforts to test the fix on our own. The problem appeared to be caused by a series of strcat() sprintf() strcpy() and other easily abused function calls however Secure Network Operations can not confirm that as fact.

Currently ListProc has been moved to SourceForge however, the status of this problem is not known. SecNetOps has not been in contact with CREN for a number of months. The current release on SourceForge has not been updated since March of 2002 so the fix is probably not available to the public. <<http://sourceforge.net/projects/listproc/>> <http://sourceforge.net/projects/listproc/> is the current home of ListProc.

Zillion from Safemode.org was able to successfully exploit this problem in a SecNetOps lab setting.

Example:

```
gentoo listproc $ head -n 12 List-Proc-catmail.pl
#!/usr/bin/perl
#
# Quick hack for the ListProc catmail overflow found by KF
(dotslash@sno soft.com)
# Written by zillion (zillion@safemode.org) on July 23, 2002
#
# Tested on version 8.2.09
#
# [zillion@ghetto lp8]$ ./expl.pl -f ./catmail
# The new return address: 0xbfffae1c
# sh-2.05# id
# uid=0(root) gid=1214(sno soft) groups=1214(sno soft),520(zillion)
```

The buffer overflow in ULISTPROC_UMASK may not be the only issues present. NetSecOps would suggest evaluating a *supported* mailing list solution.

Patch or Workaround:

```
chmod -s /path/to/catmail
```

Vendor Status:

Status is unknown. Fix was created but not distributed.

ADDITIONAL INFORMATION

Securiteam: [UNIX] ListProc Mailing List ULISTPROC_UMASK Overflow

The information has been provided by <mailto:dotslash@globalintersec.com>
KF.

=====

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.