

[UNIX] Buffer Overflow in INN's control Message Handling

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-01/0036.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/08/04

To: list@securiteam.com

Date: 8 Jan 2004 18:58:14 +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>

Buffer Overflow in INN's control Message Handling

SUMMARY

A buffer overflow has been discovered in a portion of the control message handling code introduced in INN 2.4.0. It is likely that this overflow could be remotely exploited to gain access to the user innd runs as. INN 2.3.x and earlier are not affected. The INN CURRENT tree is affected.

DETAILS

Vulnerable systems:

- * INN 2.4.0 and prior

Immune systems:

- * INN version 2.4.1

INN 2.4.1 has just been released with a fix for this issue and various other accumulated patches. We strongly urge anyone running INN 2.4.0 or any STABLE snapshot to upgrade to this version, or apply the attached patch to their source tree and reinstall with make update. There should be no incompatibilities between INN 2.4.1 and INN 2.4.0 or STABLE snapshots.

Securiteam: [UNIX] Buffer Overflow in INN's control Message Handling

ISC would like to apologize for this problem, which was caused by misuse of static buffers and a dangerous internal INN function that ISC intend to remove completely in the next stable release. The current development branch has already been converted almost entirely to strncpy, strcat, and other safe string handling routines and that conversion should be complete in the INN 2.5.0 release.

Following is a patch against INN 2.4.0. It should also apply to a current STABLE or CURRENT snapshot if you use patch -l to apply it.

```
--- inn-2.4.0/innd/art.c.orig 2003-05-04 15:10:14.000000000 -0700
+++ inn-2.4.0/innd/art.c 2004-01-07 15:25:08.000000000 -0800
@@ -1773,7 +1773,7 @@
bool
ARTpost(CHANNEL *cp)
{
- char *p, **groups, ControlWord[SMBUF], tmpbuff[32], **hops;
+ char *p, **groups, ControlWord[SMBUF], **hops, *controlgroup;
  int i, j, *isp, hopcount, oerrno, canpost;
  NEWSGROUP *ngp, **ngptr;
  SITE *sp;
@@ -2185,9 +2185,10 @@
  * or control. */
  if (IsControl && Accepted && !ToGroup) {
    ControlStore = true;
- FileGlue(tmpbuff, "control", '.', ControlWord);
- if ((ngp = NGfind(tmpbuff)) == NULL)
+ controlgroup = concat("control.", ControlWord, (char *) 0);
+ if ((ngp = NGfind(controlgroup)) == NULL)
    ngp = NGfind(ARTctl);
+ free(controlgroup);
  ngp->PostCount = 0;
  ngptr = GroupPointers;
  *ngptr++ = ngp;
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:rra@isc.org> Russ Allbery and Dan Riley.

=====

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] Buffer Overflow in INN's control Message Handling

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.