

[UNIX] Ecartis Contains Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0054.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/18/03

To: list@securiteam.com

Date: 18 Aug 2003 16:01:11 +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>

Ecartis Contains Multiple Vulnerabilities

SUMMARY

<<http://www.ecartis.org/>> Ecartis is "an open-source (GNU License) software package that administers mailing lists (similar to Majordomo and Listserv)". Several security vulnerabilities have been found in the product allowing remote attackers to execute arbitrary code, and to remotely cause the product to reveal to them the administrative password used by Ecartis' administrator.

DETAILS

Vulnerable systems:

* Ecartis version 1.0

Password disclosure:

Ecartis contains liscrypt that supports some variables and functions. User input is fully trusted in several places that allow calling those functions or viewing variables.

For example, send an email to ecartis@host.com:

subscribe secret-list

subscribe <\$post-password>

Securiteam: [UNIX] Ecartis Contains Multiple Vulnerabilities

The first command will fail, but it selects the secret-list as an active list. Second command will also fail, but the reply mail expands the post-password to the real password.

Multiple Buffer Overflows:

The product contains multiple buffer overflows. These have been fixed by the provided (unofficial) patch:

```
diff -ru ecartis-1.0.0-old/src/smtp.c ecartis-1.0.0/src/smtp.c
--- ecartis-1.0.0-old/src/smtp.c Fri Apr 18 09:45:04 2003
+++ ecartis-1.0.0/src/smtp.c Thu Aug 14 17:30:24 2003
@@ -330,18 +330,19 @@
     return 1;
 }

-void smtp_body_822bis(const char *src, char *dest)
+void smtp_body_822bis(const char *src, char *dest, size_t size)
 {
     const char *ptr1;
-    char *ptr2;
+    char *ptr2, *end;
     int lastcr;

     lastcr = 0;

     ptr1 = src;
     ptr2 = dest;
+    end = dest + size - 2;

-    while(*ptr1) {
+    while(*ptr1 && ptr2 < end) {
         if ((*ptr1 == '\n') && (!lastcr)) {
             *ptr2++ = '\r';
         } else if (*ptr1 == '\r') {
@@ -367,7 +368,7 @@
     {
         char buffer[HUGE_BUF];

-    smtp_body_822bis(line,&buffer[0]);
+    smtp_body_822bis(line,&buffer[0], sizeof(buffer));

         clean_var("smtp-last-error", VAR_TEMP);
         if (!sock_printf(my_socket,"%s",buffer)) {
@@ -385,7 +386,7 @@

         buffer_printf(buffer2, sizeof(buffer2) - 1, "%s\r\n", line);

-    smtp_body_822bis(buffer2,&buffer[0]);
+    smtp_body_822bis(buffer2,&buffer[0], sizeof(buffer));

         clean_var("smtp-last-error", VAR_TEMP);
```

Securiteam: [UNIX] Ecartis Contains Multiple Vulnerabilities

```
if (!sock_printf(my_socket,"%s",buffer)) {
diff -ru ecartis-1.0.0-old/src/unhtml.c ecartis-1.0.0/src/unhtml.c
--- ecartis-1.0.0-old/src/unhtml.c Fri Apr 18 09:45:04 2003
+++ ecartis-1.0.0/src/unhtml.c Thu Aug 14 17:43:03 2003
@@ -161,6 +161,25 @@
     case HTMLPARSE_NORMAL:
     case HTMLPARSE_EATTAG:
     {
+ /* Wordwrap */
+ if (linechars > 76) {
+ char tempbuf[1024];
+ *tptr = 0;
+
+ tptr = strrchr(linebuffer, ' ');
+ if (!tptr) tptr = strrchr(linebuffer, '-');
+ if (!tptr) tptr = &tempbuf[76];
+
+ buffer_printf(tempbuf,1023,"%s",
+ (*tptr == ' ') ? tptr + 1 : tptr);
+ *tptr = 0;
+
+ newline(outfile,&linebuffer[0],indent,linemode);
+ buffer_printf(linebuffer,79,"%s",tempbuf);
+ tptr = &linebuffer[strlen(linebuffer)];
+ linechars = strlen(linebuffer);
+ lastspace = 1;
+ }
         if (tempchar == '&') {
             memset(buffer, 0, sizeof(buffer));
             tagptr = &buffer[0];
@@ -182,25 +201,6 @@
             lastspace = (tempchar == ' ');
         }

- /* Wordwrap */
- if (linechars > 76) {
- char tempbuf[1024];
- *tptr = 0;
-
- }
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:tss@iki.fi> Timo Sirainen.

=====

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] Ecartis Contains Multiple Vulnerabilities

=====
=====

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.