

[UNIX] ARC Insecure Temporary File Creation

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0072.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/19/05

To: list@securiteam.com

Date: 19 Sep 2005 10:26:08 +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>

ARC Insecure Temporary File Creation

SUMMARY

<<http://sourceforge.net/projects/arc/>> ARC is "used to create and maintain file archives. An archive is a group of files collected together into one file in such a way that the individual files may be recovered intact".

A vulnerability in ARC is caused due to temporary file being created insecurely. The temporary file used for archive creation could be read by untrusted users.

DETAILS

Vulnerable Systems:

* ARC versions 5.21j and prior.

Vulnerable code:

arc.c :

```
210 /* see where temp files go */
```

```
211 #if !_MTS
```

```
212 arctemp = calloc(1, STRLEN);
```

```
213 if (!(arctemp2 = envfind("ARCTEMP")))
```

```
214 arctemp2 = envfind("TMPDIR");
```

Securiteam: [UNIX] ARC Insecure Temporary File Creation

```
215 if (arctemp2) {
216 strcpy(arctemp, arctemp2);
217 n = strlen(arctemp);
218 if (arctemp[n - 1] != CUTOFF)
219 arctemp[n] = CUTOFF;
220 }
221 #if UNIX
222 else strcpy(arctemp, "/tmp/");
223 #endif
224 #if !MSDOS
225 {
226 static char tempname[] = "Axxxxxxx";
227 strcat(arctemp, mktemp(tempname));
228 }
229 #else
230 strcat(arctemp, "$ARCTEMP");
231 #endif
232 #else
233 guinfo("SHFSEP ", gotinf);
234 sepchr[0] = gotinf[0];
235 guinfo("SCRFCHAR", gotinf);
236 tmpchr[0] = gotinf[0];
237 arctemp = "-$$$";
238 arctemp[0] = tmpchr[0];
239 #endif
240 arctemp2 = NULL;
241
242 #if !UNIX
243 /* avoid any case problems with arguments */
244
245 for (n = 1; n < num; n++) /* for each argument */
246 upper(arg[n]); /* convert it to uppercase */
247 #else
248 /* avoid case problems with command options */
249 upper(arg[1]); /* convert to uppercase */
250 #endif
251
252 /* create archive names, supplying defaults */
253 #if UNIX
254 if (!stat(arg[2], &sbuf)) {
255 if ((sbuf.st_mode & S_IFMT) == S_IFDIR)
256 makefnam(arg[2], ".arc", arcname);
257 else
258 strcpy(arcname, arg[2]);
259 } else
260 makefnam(arg[2], ".arc", arcname);
261 #else
262 makefnam(arg[2], ".ARC", arcname);
263 #endif
```

Securiteam: [UNIX] ARC Insecure Temporary File Creation

Take a look on a the right off temporary files in /tmp :
-rw-r--r-- 1 root root 1564 Sep 5 10:28 A3C6Zs4.arc
The file should not be world readable.

The same problem exists in marc.c

ADDITIONAL INFORMATION

The information has been provided by <mailto:exploits@zataz.net> ZATAZ Audits.

The original article can be found at:

<<http://www.zataz.net/adviso/arc-09052005.txt>>

<http://www.zataz.net/adviso/arc-09052005.txt>

=====

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.