# Bug fixes inside curl

Certain salient bugs and deficiency with features have to be dealt with for curl to be usable in Infa. Following are a description for the same.

Spnego Free bug:-

Inside the cleanup method of http\_negotiate.c the correct free strategy is:-

#ifdef HAVE\_SPNEGO

Curl\_safefree(neg\_ctx->output\_token.value);

#else

if(neg\_ctx->output\_token.value)

gss\_release\_buffer(&minor\_status, &neg\_ctx->output\_token);

#endif /\*HAVE\_SPNEGO\*/

Earlier only gss\_release\_buffer was being used for all types of auth protocols (including both Spnego and standard GSS API. Consumer should also look for other gss\_release\_buffers within the same file and appropriately introduce the same logic. Without this change, Curl will outrightly crash in Spnego mode.

Arbitrary SPN bug:-

Without this change, Curl will never be able to take arbitrary SPNs. Modify get\_gss\_name function inside http\_negotiate.c to include the following code:-

if(conn->bits.service\_principal) {

token.value = conn->service\_principal;

token.length = strlen(conn->service\_principal) + 1;

major\_status = gss\_import\_name(&minor\_status, &token,

(gss\_OID) GSS\_C\_NT\_USER\_NAME , server);

return GSS\_ERROR(major\_status) ? -1 : 0;

}

Warning – The last time I tried pushing this change, a very similar option was being advocated by another developer in the curl forums so I don’t know if this will be required in future releases or not.

Junk string for enabling authentication bug:-

Earlier negotiate authentication happened if some junk string was provided in username curloption. Moreover this string was ignored and SSO was used always. This is unacceptable since there would be no way to do auth without junk It’s also called bug 440 in the curl community. In order to resolved this, inside Curl\_http\_output\_auth function of http.c the following change was made.

/\*commented to solve bug 440 in curl

\*

\*if((conn->bits.httpproxy && conn->bits.proxy\_user\_passwd) ||

\* conn->bits.user\_passwd)

\* continue please

\*else {

\* authhost->done = TRUE;

\* authproxy->done = TRUE;

\* return CURLE\_OK; //no authentication without username/password

\*}

\*/