Bug 5104 - Memory leak in RFC 2169 response parsing

Status:	RESOLVED FIXED	**Reported:**	2021-02-22 06:55 UTC by Joshua Rogers
Alias:	None	**Modified:**	2021-05-19 13:55 UTC (History)
		CC List:	0 users
Product:	Squid		
Component:	other (show other bugs)	**See Also:**	
Version:	unspecified	**Browser:**	---
Hardware:	All All	**Fixed Versions:**	4.15, 5.0.6
Importance:	P5 blocker		
Assignee:	SQUID BUGS ALIAS		
URL:			
Depends on:			
Blocks:			

Attachments

Add an attachment (proposed patch, testcase, etc.)

Note

You need to log in before you can comment on or make changes to this bug.

Joshua Rogers 2021-02-22 06:55:38 UTC Description

```
Hi there,

In src/urn.cc, there is a small memory leak in the function urnParseReply(const
char *inbuf, const HttpRequestMethod& m):

    char *buf = xstrdup(inbuf);


'buf' here is never freed.
```

Alex Rousskov 2021-02-22 22:59:21 UTC Comment 1

```
Thank you for reporting this bug.

We can just free the buffer after the loop AFAICT, but, ideally, that leaking
buffer should be converted into SBuf, and the tokenizing loop iterating that buffer
should be converted to use an SBuf Tokenizer.

Alternatively, the whole URN-handling code can be removed as too risky and
neglected.

Quality fixes welcome!
```

Alex Rousskov 2021-02-22 23:02:08 UTC Comment 2

```
Amos created a PR with the simple solution: https://github.com/squid-
cache/squid/pull/778
```

Amos Jeffries 2021-03-29 09:53:16 UTC Comment 3

```
PR merged
```