

# [UNIX] Squid's ICAP Implementation Lacks Defer Check When Reading From ICAP Server

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-12/msg00028.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 11 Dec 2007 15:16:17 +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>

-----

Squid's ICAP Implementation Lacks Defer Check When Reading From ICAP Server

---

## SUMMARY

A vulnerability in Squid's ICAP implementation allows attackers to cause Squid to consume large amounts of memory.

## DETAILS

Vulnerable Systems:

- \* Squid version 2.5
- \* Squid version 2.6

Squid's ICAP implementation does not check mem-store size before reading from an ICAP-server. If the user does not confirm browsers download-message-box, Squid keeps on reading data from the ICAP server into the memory store, whilst no more data can be delivered to the client. Thus the memory store is growing and Squid may – in worst case – consume memory up to the size of the users download.

Patch:

diff -Naur squid-2.5.STABLE10.ICAP.orig/src/icap\_respmod.c

## [UNIX] Squid's ICAP Implementation Lacks Defer Check When Reading From ICAP Server

```
squid-2.5.STABLE10.ICAP/src/icap_respmod.c
--- squid-2.5.STABLE10.ICAP.orig/src/icap_respmod.c 2007-12-07
08:48:14.124859537 +0100
+++ squid-2.5.STABLE10.ICAP/src/icap_respmod.c 2007-12-07
08:49:23.501573696 +0100
@@ -49,6 +49,7 @@
static int icapReadReply2(IcapStateData * icap);
static void icapReadReply3(IcapStateData * icap);
static void write_av_stat(char *virus, char *statsrc, char *statdst);
+static int icapCheckDeferRead(int fd, void *data);

#define EXPECTED_ICAP_HEADER_LEN 256
const char *crlf = "\r\n";
@@ -415,7 +416,7 @@
ErrorState *err;
const char *start;
const char *end;
-
+
debug(81, 5) ("icapRespModReadReply: FD %d data = %p\n", fd, data);
statCounter.syscalls.sock.reads++;

@@ -1100,6 +1102,7 @@
} else if (!icap->flags.no_content) {
/* Wait for EOF condition */
commSetSelect(fd, COMM_SELECT_READ, icapReadReply, icap, 0);
+ commSetDefer(fd, icapCheckDeferRead, icap);
debug(81,
3)
("icapReadReply3: Going to read mode data throught
icapReadReply\n");
@@ -1134,3 +1137,27 @@
strcat(subsrvProto, statsrc);
send_service_stat(rid, 10, avServer, avService, subsrvProto, virus,
statdst, 0, 1, featured);
}
+
+static int
+icapCheckDeferRead(int fd, void *data)
+{
+ IcapStateData *httpState = data;
+ StoreEntry *e = httpState->respmod.entry;
+ MemObject *mem = e->mem_obj;
+
+ int rc=0;
+
+ if (EBIT_TEST(e->flags, ENTRY_FWD_HDR_WAIT))
+ return rc;
+ if (EBIT_TEST(e->flags, RELEASE_REQUEST)) {
+ if (mem->inmem_hi - mem->inmem_lo > SM_PAGE_SIZE +
Config.Store.maxInMemObjSize + READ_AHEAD_GAP){
```

## [UNIX] Squid's ICAP Implementation Lacks Defer Check When Reading From ICAP Server

```
+ debug(81, 5) ("icapCheckDeferRead: Defering read\n");
+ return 1;
+ }
+ }
+ if (mem->inmem_hi - storeLowestMemReaderOffset(e) > READ_AHEAD_GAP){
+ debug(81, 5) ("icapCheckDeferRead: Defering read\n");
+ return 1;
+ }
+ return 0;
+}
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:m.huter@xxxxxxxxxx>> Martin Huter.

The original article can be found at:

<[http://www.squid-cache.org/bugs/show\\_bug.cgi?id=2136](http://www.squid-cache.org/bugs/show_bug.cgi?id=2136)>

[http://www.squid-cache.org/bugs/show\\_bug.cgi?id=2136](http://www.squid-cache.org/bugs/show_bug.cgi?id=2136)

=====

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@xxxxxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxxxxx](mailto:list-subscribe@xxxxxxxxxxxxxxxx)

=====

=====

### 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.