README.md

Exim heap overflow in host_name_lookup()

Another issue, which has been silently fixed in 4.95

https://github.com/Exim/exim/commit/d4bc023436e4cce7c23c5f8bb5199e178b4cc743

Details:

```
int
host_name_lookup(void)
{
....
[1]    int count = 0;
      int old_pool = store_pool;

      sender_host_dnssec = dns_is_secure(dnsa);
      store_pool = POOL_PERM;        /* Save names in permanent storage */

      for (dns_record * rr = dns_next_rr(dnsa, &dnss, RESET_ANSWERS);
           rr;
           rr = dns_next_rr(dnsa, &dnss, RESET_NEXT)) if (rr->type == T_PTR)
        count++;
```

```
[2]      aptr = sender_host_aliases = store_get(count * sizeof(uschar *), FALSE);


       for (dns_record * rr = dns_next_rr(dnsa, &dnss, RESET_ANSWERS);
           rr;
           rr = dns_next_rr(dnsa, &dnss, RESET_NEXT)) if (rr->type == T_PTR)
        {
        uschar * s = store_get(ssize, TRUE);    /* names are tainted */

        /* If an overlong response was received, the data will have been
        truncated and dn_expand may fail. */

        if (dn_expand(dnsa->answer, dnsa->answer + dnsa->answerlen,
             US (rr->data), (DN_EXPAND_ARG4_TYPE)(s), ssize) < 0)
          {
          log_write(0, LOG_MAIN, "host name alias list truncated for %s",
            sender_host_address);
          break;
          }

        store_release_above(s + Ustrlen(s) + 1);
        if (!s[0])
          {
          HDEBUG(D_host_lookup) debug_printf("IP address lookup yielded an "
            "empty name: treated as non-existent host name\n");
          continue;
          }
[3]       if (!sender_host_name) sender_host_name = s;
        else *aptr++ = s;
        while (*s) { *s = tolower(*s); s++; }

[4]      *aptr = NULL;            /* End of alias list */
      store_pool = old_pool;   /* Reset store pool */

      /* If we've found a name, break out of the "order" loop */

      if (sender_host_name) break;
      }
```

On line #2, array for 'count' entries will be allocated.
If on line #3 sender_host_name is not NULL, entry to this array will be written.
This for loop, writes exactly 'count' entries in this case.
On line #4 oob write occurs.

To trigger the issue, we need to make Exim call host_name_lookup() with
sender_host_name != NULL.
It is possible to do for instance, if we add global configuration entry,
which is using '$sender_host_name' variable.

```
host_name_lookup() will be called twice - first when Exim tries to expand
$sender_host_name,
second in smtp_start_session() (smtp_in.c)

To reproduce it on Ubuntu with exim4 package install,
i'd recomment to use included exim.conf and just run exim as:
# exim -bd -d -C /etc/exim4/exim.conf


1. Edit exim config file, add the following lines at the beginning :
host_lookup = *
message_size_limit      = ${if def:sender_host_name {32M}{32M}}

4. Run exim:
#./build-Linux-x86_64/exim -bd -d

5. Run authorizative dns server for example.com

6. Send email to your exim server
```

Asan log attached.

Releases

No releases published

Packages

No packages published