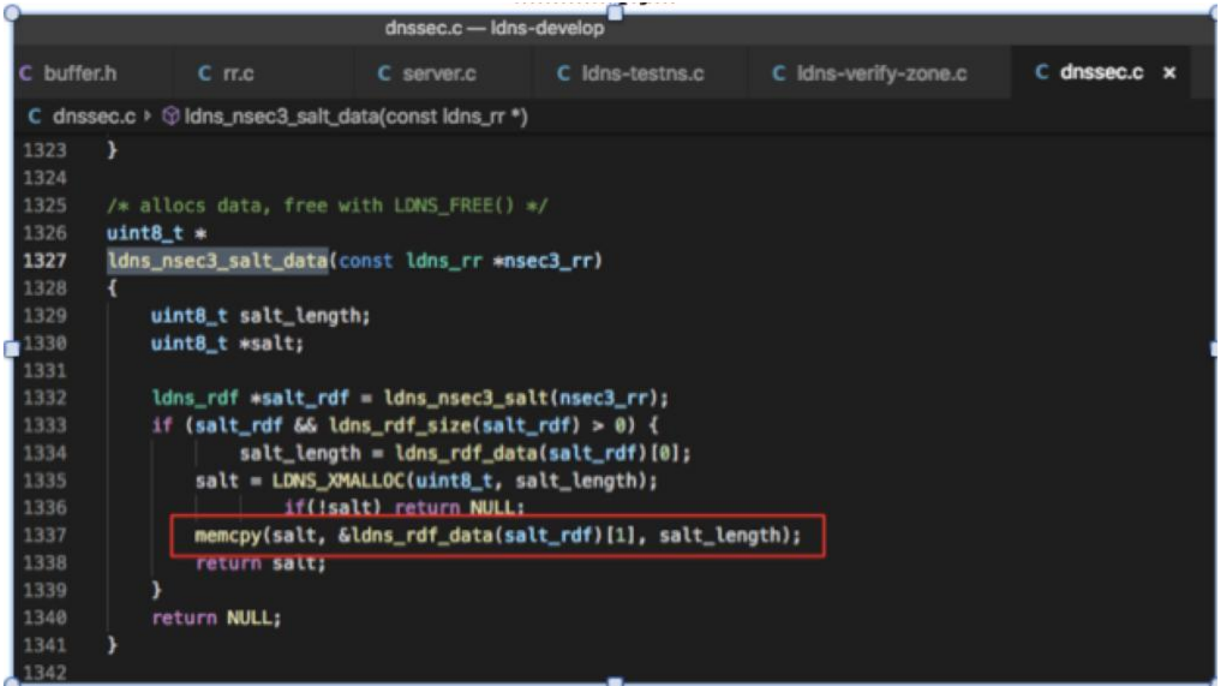
Heap Out-of-bound Read vulnerability #51

Closed **pokerfacett** opened this issue on Sep 25, 2019 · 4 comments

pokerfacett commented on Sep 25, 2019 • edited

Description:

When the zone file is parsed, the function ldns_nsec3_salt_data is too trusted for the length value obtained from the zone file. When the memcpy is copied, the 0xfe - ldns_rdf_size(salt_rdf) byte data can be copied, causing heap information leakage.
Vulnerability location:



```
}

/* allocs data, free with LDNS_FREE() */
uint8_t *
ldns_nsec3_salt_data(const ldns_rr *nsec3_rr)
{
    uint8_t salt_length;
    uint8_t *salt;

    ldns_rdf *salt_rdf = ldns_nsec3_salt(nsec3_rr);
    if (salt_rdf && ldns_rdf_size(salt_rdf) > 0) {
            salt_length = ldns_rdf_data(salt_rdf)[0];
        salt = LDNS_XMALLOC(uint8_t, salt_length);
                if(!salt) return NULL;
        memcpy(salt, &ldns_rdf_data(salt_rdf)[1], salt_length);
        return salt;
    }
    return NULL;
}
```

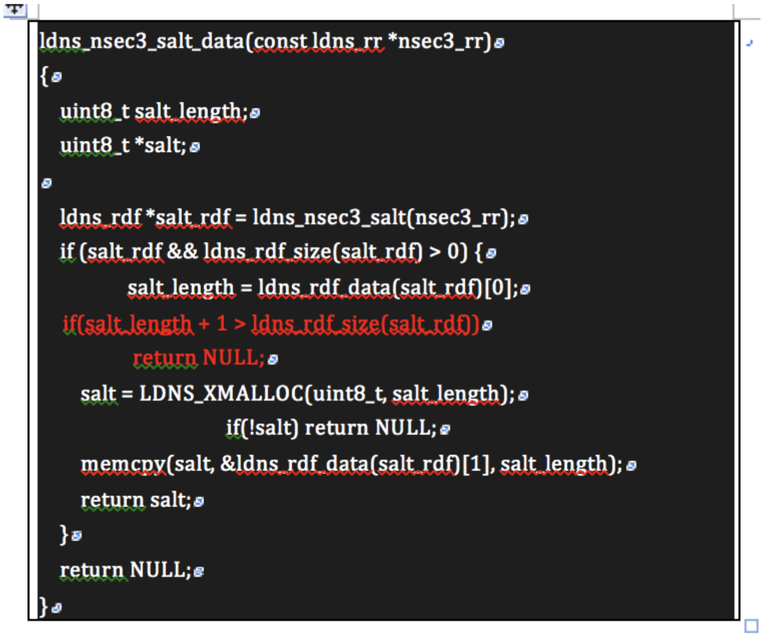
fuzz log:

INFO-w100wcrash.docx

fuzz payload:

w100wcrash-8f078e69e2781bbc4811a12d51df1c8674672306.txt

Repaire Suggestion:



```
ldns_nsec3_salt_data(const ldns_rr *nsec3_rr)
{
  uint8_t salt_length;
  uint8_t *salt;

  ldns_rdf *salt_rdf = ldns_nsec3_salt(nsec3_rr);
  if (salt_rdf && ldns_rdf_size(salt_rdf) > 0) {
          salt_length = ldns_rdf_data(salt_rdf)[0];
   if(salt_length + 1 > ldns_rdf_size(salt_rdf))
           return NULL;
     salt = LDNS_XMALLOC(uint8_t, salt_length);
                    if(!salt) return NULL;
     memcpy(salt, &ldns_rdf_data(salt_rdf)[1], salt_length);
     return salt;
  }
  return NULL;
}
```

wcawijngaards added a commit that referenced this issue on Sep 26, 2019

`* bugfix #51: Heap Out-of-bound Read vulnerability in` ⋯ 136ec42

wcawijngaards commented on Sep 26, 2019 Member

Thanks! I applied your suggestion (with a cast to size_t to make the 255 case and also compiler signedness warnings work).

wcawijngaards closed this as completed on Sep 26, 2019

pokerfacett commented on Jun 5, 2020 Author

> Thanks! I applied your suggestion (with a cast to size_t to make the 255 case and also compiler signedness warnings work).

hi ,could you report this in security advisory and help to request a CVE for us:https://help.github.com/cn/github/managing-security-vulnerabilities/publishing-a-security-advisory

wtoorop commented on Jun 8, 2020 Member

Hi **@pokerfacett** , we don't think a CVE is necessary, but we will work to a release with the issue fixed on a short term.

pokerfacett commented on Jan 22 Author

CVE-2020-19861 was assigned for this issue

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants