New issue   Jump to bottom

heap Out-of-bound Read vulnerability #50

⊘ Closed   **pokerfacett** opened this issue on Sep 24, 2019 · 6 comments

---

pokerfacett commented on Sep 24, 2019

ldns heap Out-of-bound Read.pdf

✎ 👤 **pokerfacett** changed the title ~~heap Out-of-bound Read~~ heap Out-of-bound Read vulnerability on Sep 24, 2019

👤 **wcawijngaards** closed this as completed in `332e705` on Sep 24, 2019

---

wcawijngaards commented on Sep 25, 2019   Member

Sorry the notices did not make it here.

Commits `15d9620` and `4e98615` are there to fix the problem.

Do they fix the problem for you? They pull in fixes for the code that you notice the failure in, and I think that probably fixes the flaw.

✉ **wcawijngaards** commented on Sep 25, 2019   Member

Hi!

Thanks for the report, I looked at the code and committed fixes for it
yesterday, but my colleague (Willem) just had to go home at that time.
Hence the commits arrived, but not replies to the email.

The commits are similar to Unbound's code for it, and I think they fix
the problem, as they test for out-of-bounds on the lines where the
out-of-bounds is reported. So I put the text 'fix' in the commit
message, and this auto-closes the issue ticket on github.

Best regards, Wouter
　…

---

pokerfacett commented on Sep 25, 2019   Author

ok，thanks

---

pokerfacett commented on Jun 5, 2020   Author

> Hi! Thanks for the report, I looked at the code and committed fixes for it yesterday, but my colleague (Willem) just had to go home at that time. Hence the commits arrived, but not replies to
> the email. The commits are similar to Unbound's code for it, and I think they fix the problem, as they test for out-of-bounds on the lines where the out-of-bounds is reported. So I put the text
> 'fix' in the commit message, and this auto-closes the issue ticket on github. Best regards, Wouter
> …
> On 25/09/2019 06:58, 三胖子 wrote: Why closed？？ — You are receiving this because you modified the open/close state. Reply to this email directly, view it on GitHub <#50?
> email_source=notifications&email_token=ABH2RT6GEVWERYJRNV6OVCTQLLVZHA5CNFSM4IZ4IWOKYY3PNVWWK3TUL52HS4DFVREXG43VMVBW63LNMVXHJKTDN5WW2ZLOORPWSZGOD7
> QTFPY#issuecomment-534852287>, or mute the thread https://github.com/notifications/unsubscribe-auth/ABH2RT5YIWWIMCMIR5XCNNDQLLVZHANCNFSM4IZ4IWOA.

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.

---

ajakk commented on Jan 21

> 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

You don't need to be an upstream to request a CVE from MITRE. Someone requested one for this and CVE-2020-19860 was assigned.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants