[Dnsmasq-discuss] Security - IMPORTANT

Simon Kelley simon at thekelleys.org.uk
Mon May 11 17:18:25 UTC 2026

- Previous message (by thread): [Dnsmasq-discuss] Issue with circuit-id matching on dhcp requests
- Next message (by thread): [Dnsmasq-discuss] Malformed RRSIG Can Crash dnsmasq
- **Messages sorted by:** [date] [thread] [subject] [author]

Today, 11th May 2026 CERT is releasing a set of six CVEs for serious
security vulnerabilities in dnsmasq. These are all long-standing bugs
which apply to pretty much all non-ancient versions. The CVE has been
pre-disclosed to vendors, so hopefully they will be releasing patched
versions of their dnsmasq packages in a timely manner.

Details and patches are available on the website at

https://thekelleys.org.uk/dnsmasq/CVE/

and I have made "2.92rel2" release of the current 2.92 dnsmasq stable
release which is downloadable from the usual place and has had these
patches applied.

At the same time, the commits which fix these bugs in the development
tree will be uploaded. Some of these use the same patches as the
backports, but some are more comprehensive re-writes to tackle root-causes.

There has been something of a revolution in AI-based security research,
and I've spent a lot of time over the last couple of months dealing with
bug reports, weeding duplicates (so many duplicates!) and triaging bugs
into those which need vendor pre-disclosure and those which it's better
to make public and fix immediately. Those judgements have been
necessarily subjective, but given the number of times "good guys" have
found these bugs, there's no doubt that "bad guys" have been able to do
the same, so long embargoes seem kind of pointless. There's also the
problem that the amount of time and effort, for all actors, needed to
co-ordinate an embargo and provide backports is huge. I think the
priority for most bugs is to fix them going forward, and have new
dnsmasq releases as bug-free as possible. To this end, you may have
noticed that there have been a lot of security-fix commits to the git
repo in the weeks prior to this announcement.

I will shortly tag dnsmasq-2.93rc1 and the aim is to get a stable 2.93
release done ASAP. Testing of release candidate by members here is
important and I'd like to encourage anyone who can to do that as soon as
they can. With luck, 2.93 could be out in a week or so.

The tsunami of AI-generated bug reports shows no signs of stopping, so
it is likely that this process will have to be repeated again soon.
There's a tension between getting as much as possible of the ongoing bug
stream fixed in 2.93 and it's timely release. I plan to prioritise
timeliness, and keep working after that as necessary.

Simon.

- Previous message (by thread): [Dnsmasq-discuss] Issue with circuit-id matching on dhcp requests
- Next message (by thread): [Dnsmasq-discuss] Malformed RRSIG Can Crash dnsmasq
- **Messages sorted by:** [date] [thread] [subject] [author]

More information about the Dnsmasq-discuss mailing list