Patching Nameservers: Austria reacts to VU#800113

Update to CERT.at Report #2

www.cert.at <team@cert.at>

Otmar Lendl <lendl@cert.at>

July 28, 2008

Update as of Monday, July 28th

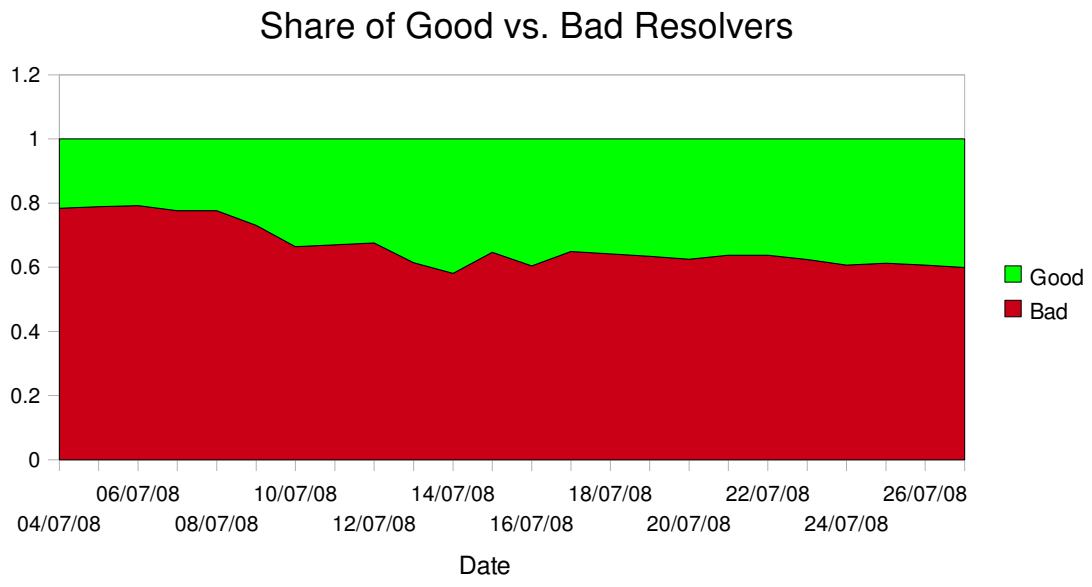
We published our report on Thursday, July 24th which included measurements up to July 21st.

Press coverage was good in Austria (and we even made Slashdot), and we managed to alert a few operators via our channels.

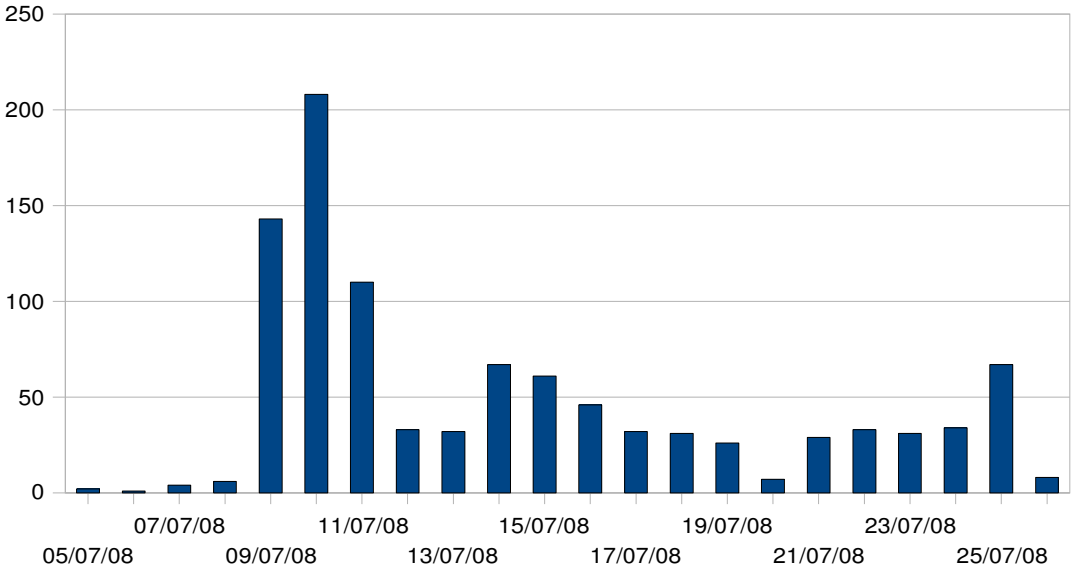
So we had good reasons to hope that numbers would improve over the weekend.

Here is the reality-check:

Good vs. bad resolvers



When did people patch?

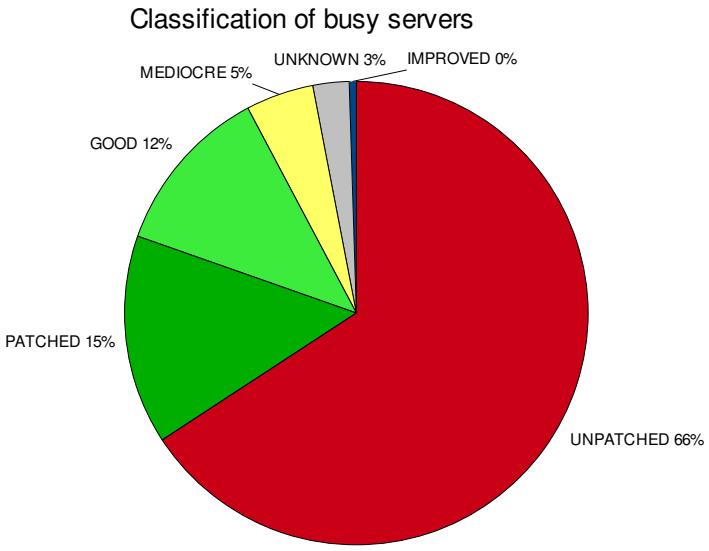


The data here is not complete, as we want to see more than just one day with clear improvement before we consider a resolver to be successfully patched.

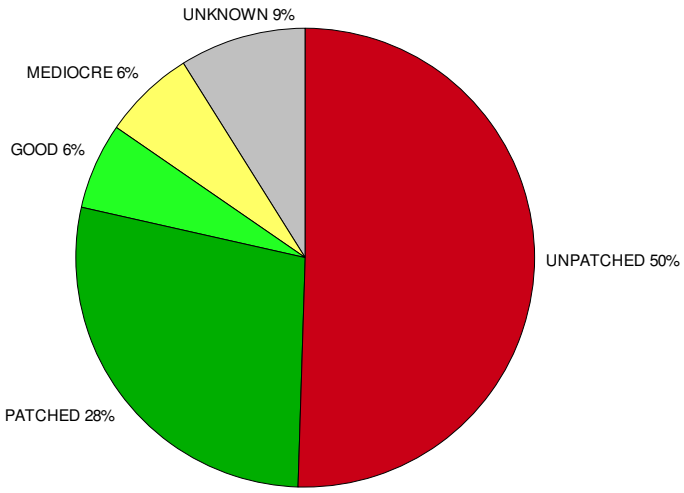
Classification

Last week we wrote:

> Our datasets covers 18 days, four of which were weekend. Looking at all servers which appear in at least 14 days, we find the following classification:
>
> Roughly speaking, one quarter of all relevant resolvers implement source port randomization now, whereas the vast majority does not.



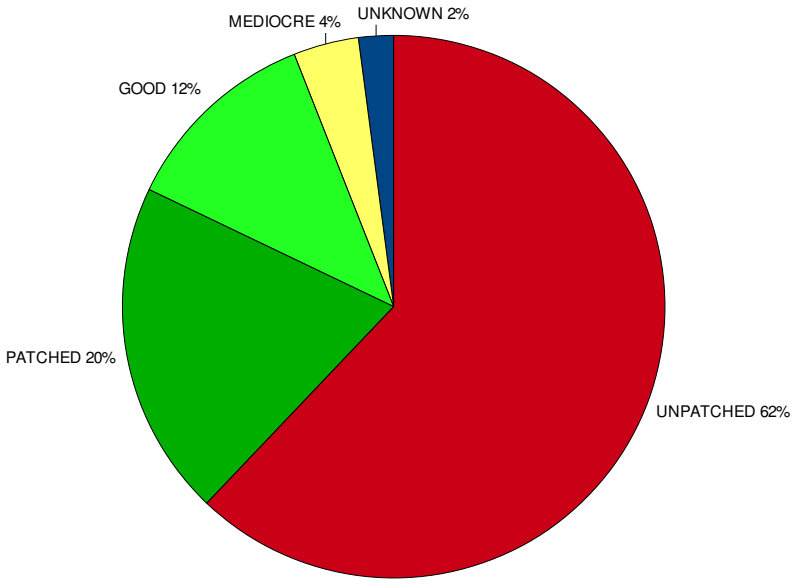
Weighting resolvers based on the number of queries shows a slightly better picture:



About half of all DNS queries are made by unpatched resolvers and thus are vulnerable to DNS cache poisoning.

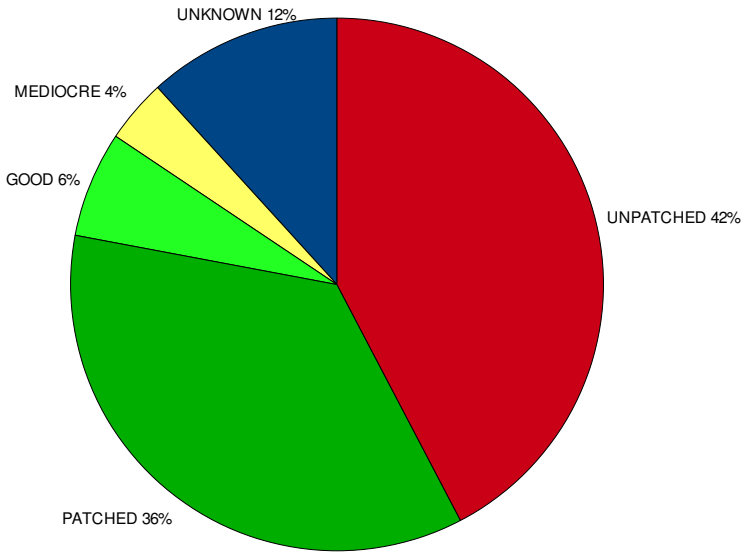
Using data from up to and including Sunday 27th, we now find:

All busy resolvers:



This is slightly better.

Weighted by queries



Whereas the overall percentage of patched resolvers decreased just a bit (66 → 62 %), the weighted queries showed twice as much improvement.

Summary

Yes, there has been steady improvement, but the patch rate is still low.

Regrettably, it still looks like there will be a successful and highly publicized attack before the rest of the resolvers get patched.