Date: Fri, 27 Aug 2021 16:09:34 +0800
From: butt3rflyh4ck <butterflyhuangxx@...il.com>
To: oss-security@...ts.openwall.com
Subject: Re: Linux kernel: qrtr: another out-of-bound Read in
 qrtr_endpoint_post in net/qrtr/qrtr.c

Hi, Red Hat has assigned CVE-2021-3743 to this issue.

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3743

Regards,
   butt3rflyh4ck.

On Fri, Aug 27, 2021 at 1:51 PM butt3rflyh4ck
<butterflyhuangxx@...il.com> wrote:
>
> The patch is available upstream.
> https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=7e78c597c3ebfd0cb329aa09a838734147e4f117
>
> Regards,
> butt3rflyh4ck.
>
>
> On Wed, Aug 25, 2021 at 10:40 AM butt3rflyh4ck
> <butterflyhuangxx@...il.com> wrote:
> >
> > Hi, There was another out-of-bound read bug in qrtr_endpoint_post in
> > net/qrtr/qrtr.c in 5.14.0-rc6+ and reproduced it.
> >
> > This check in qrtr_endpoint_post was incomplete, did not consider size is 0:
> > ```
> > if (len != ALIGN(size, 4) + hdrlen)
> >                goto err;
> > ```
> > if size from qrtr_hdr is 0, the result of ALIGN(size, 4) will be 0,
> > In case of len == hdrlen and size == 0 in header this check won't fail and
> > ```
> >  if (cb->type == QRTR_TYPE_NEW_SERVER) { /* Remote node endpoint can
> > bridge other distant nodes */
> >              const struct qrtr_ctrl_pkt *pkt = data + hdrlen;
> >              qrtr_node_assign(node, le32_to_cpu(pkt->server.node));
> >  }
> > ```
> > will also read out of bound from data, which is hdrlen allocated block.
> >
> >
> > #analyze and some details
> > https://lists.openwall.net/netdev/2021/08/17/124
> >
> > #patch
> > https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net.git/commit/?id=7e78c597c3eb
> > now not available upstream.
> >
> > #Timeline
> > *2021/8/17 - Vulnerability reported to netdev@...r.kernel.org.
> > *2021/8/20 - Vulnerability confirmed and patched.
> > *2021/8/23 - Vulnerability reported to secalert@...hat.com.
> > *2021/8/25 - Opened on oss-security@...ts.openwall.com.
> >
> > #Credit
> > Active Defense Lab of Venustech.
> >
> >
> > Regards,
> > butt3rflyh4ck.
> >
> > --
> > Active Defense Lab of Venustech
>
>
>
> --
> Active Defense Lab of Venustech

--
Active Defense Lab of Venustech