Subject: Re: [PATCH][ICMP]: Dst entry leak in icmp_send host re-lookup code (v2).
Posted by Herbert Xu on Tue, 01 Apr 2008 12:15:32 GMT
View Forum Message <> Reply to Message

On Wed, Mar 26, 2008 at 12:25:40PM +0300, Pavel Emelyanov wrote:
> Commit 8b7817f3a959ed99d7443afc12f78a7e1fcc2063 ([IPSEC]: Add ICMP host
> relookup support) introduced some dst leaks on error paths: the rt
> pointer can be forgotten to be put. Fix it bu going to a proper label.

I just remembered that we have exactly the same code path in IPv6
and sure enough it also has the same bug.

[IPV6]: Fix ICMP relookup error path dst leak

When we encounter an error while looking up the dst the second
time we need to drop the first dst. This patch is pretty much
the same as the one for IPv4.

Signed-off-by: Herbert Xu <herbert@gondor.apana.org.au>

Thakns,
--
Visit Openswan at http://www.openswan.org/
Email: Herbert Xu ~{PmV>HI~} <herbert@gondor.apana.org.au>
Home Page: http://gondor.apana.org.au/~herbert/
PGP Key: http://gondor.apana.org.au/~herbert/pubkey.txt
--
diff --git a/net/ipv6/icmp.c b/net/ipv6/icmp.c
index 121d517..f204a72 100644
--- a/net/ipv6/icmp.c
+++ b/net/ipv6/icmp.c
@@ -436,10 +436,10 @@ void icmpv6_send(struct sk_buff *skb, int type, int code, __u32 info,
  }

  if (xfrm_decode_session_reverse(skb, &fl2, AF_INET6))
- goto out;
+ goto out_dst_release;

  if (ip6_dst_lookup(sk, &dst2, &fl))
- goto out;
+ goto out_dst_release;

  err = xfrm_lookup(&dst2, &fl, sk, XFRM_LOOKUP_ICMP);
  if (err == -ENOENT) {