Subject: Re: [PATCH][ICMP]: Dst entry leak in icmp_send host re-lookup code (v2).
Posted by davem on Thu, 03 Apr 2008 20:00:36 GMT
View Forum Message <> Reply to Message

From: Herbert Xu <herbert@gondor.apana.org.au>
Date: Wed, 2 Apr 2008 20:40:24 +0800

> [ICMP]: Ensure that ICMP relookup maintains status quo
>
> The ICMP relookup path is only meant to modify behaviour when
> appropriate IPsec policies are in place and marked as requiring
> relookups. It is certainly not meant to modify behaviour when
> IPsec policies don't exist at all.
>
> However, due to an oversight on the error paths existing behaviour
> may in fact change should one of the relookup steps fail.
>
> This patch corrects this by redirecting all errors on relookup
> failures to the previous code path. That is, if the initial
> xfrm_lookup let the packet pass, we will stand by that decision
> should the relookup fail due to an error.
>
> This should be safe from a security point-of-view because compliant
> systems must install a default deny policy so the packet would'nt
> have passed in that case.
>
> Many thanks to Julian Anastasov for pointing out this error.
>
> Signed-off-by: Herbert Xu <herbert@gondor.apana.org.au>

Applied, thanks Herbert.