

Re: Potential hole in Ettercap 0.6.2

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/vuln-dev/2001-12/0055.html>

From: Blue Boar (BlueBoar@thievco.com)

Date: 12/04/01

Date: Tue, 04 Dec 2001 12:37:30 -0800
From: Blue Boar <BlueBoar@thievco.com>
To: Michal Zalewski <lcantuf@coredump.cx>

Michal Zalewski wrote:

>
> *GOBBLES is a good, one-time joke gone annoying... This guy is certainly a
> good english speaker – the nature of "mistakes" made by him are not ones
> newbies do; people with poor English skills tend to traslate idioms or
> grammar constructions literally, to use the incorrect meaning of a word,
> to use synonyms in their language that are not synonyms in English, to
> make _certain_ spelling mistakes and such. Actually, he either knows
> English very good (I guess better than me), or, more likely, is a native
> English speaker.*

Which is frankly why the first couple of messages were let through.
Long-time subscribers will be aware that I'm not opposed to a good joke
on list now and then.

> *He personally attacks AtStake, Alfred Huger and many
> other people,*

Which is why I have a policy against personal attacks on the list. If
I want someone's info on the list, and I can't tolerate their rants,
I'll simply summarize their info myself. This is the first time
I've had to do this in the over 2 years that the list has existed.

> *so apparently has a good knowledge of the community. This
> might be a way of someone to disclose some less revelant findings and have
> some fun. One way or another, I can hardly say any of GOBBLES advisories
> so far had a real value. I must say I do not find this offensive style
> entertaining, and I do not perceive it as something clever. Anyone
> familiar with the Usenet should have a good idea what a troll is, and how
> to deal with it... GOBBLES posts are written exclusively to cause endless
> discussions, flame wars, unnecessary noise – or, to be short, to get some
> attention.*

I'm certainly aware of what a troll is. BTW, pointing out that something
is a troll is also feeding the trolls. :) The fact that something
is a troll won't necessarily disqualify it for inclusion. It's

SecurityFocus Vuln-Dev: Re: Potential hole in Ettercap 0.6.2

pretty pointless to troll a moderated list. You generally just piss off the moderator, who is the one you have to get past.

>
> *I hate to say so, but maybe it is time to ignore him? Instead of*
> *forwarding posts or excerpts or notification about yet another*
> *vulnerability in a discontinued line of scientific calculators,*
> *command-line buffer overflow / format string bug in a program that is not*
> *supposed to be setuid, claims that a failure to log authentication failure*
> *is a "remote root exploit", or an advisory on data leak as relevant to the*
> *security of your system as disclosing your system time or username by*
> *Sendmail in mail headers? I am not saying we should ignore valuable*
> *research if it does not conform to some "style guidelines", or that we*
> *should reject such very minor (and often unverified) bug reports if*
> *described in an acceptable manner, but if it does not have any value and*
> *lacks style, it is just sad.*

Were this Bugtraq, the posts wouldn't be (and aren't) permitted. Since it's vuln-dev, I will allow some posts which I know (or think I know) aren't anything that can be exploited. I get surprised sometimes. Since we've spent a bit of time discussing *getty problems lately, it would be a bit inconsistent for me to just ignore the ettercap thing, since it appears to be just slightly more likely to have an exploitable scenario.

Along those lines, I have taken a vote in the past and have had subscribers indicate that they wish to see bugs in non-suid programs. The volume gets a bit high, though. I'll probably have to start collecting summaries for all of the "x is vulnerable" posts, similar to what Bugtraq does sometimes. I can't do it exactly like that, since this is a discussion list. I will need to let through posts that are related, but not quite the same, more often.

BB

-
- **Previous message:** [Blue Boar: "*getty \(stopping thread\)"](#)
 - **In reply to:** [Michal Zalewski: "Re: Potential hole in Ettercap 0.6.2"](#)
 - **Next in thread:** [Jonathan Bloomquist: "Re: Potential hole in Ettercap 0.6.2"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)