

Re: IDS recommendations

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ids/2001-12/0039.html>

From: Jeff Nathan (jeff@wwti.com)

Date: 12/05/01

Date: Wed, 05 Dec 2001 11:12:35 -0800
From: Jeff Nathan <jeff@wwti.com>
To: Nate.Duzenberry@mortgage.wellsFargo.COM

Nate.Duzenberry@mortgage.wellsFargo.COM wrote:

- >
- > *OOPS. I am now aware that they ported it.*
- >
- > *It still is not a good HID solution for our environment. I can't attach a*
- > *service level agreement to an open source application that doesn't have*
- > *escalation support. Not to mention that I can't put Beta software in a*
- > *production server farm! We are using it for NID in a few select scenario's*
- > *and have had problems with HP ITO integration.*
- >
- > *Sorry, those are simply the facts in a large environment.*

I'm writing this from my personal email address but I'm also in a position where I deal with a large enterprise, one that's a bit higher on fortune's list than Wells Fargo I might add and by no means small. There is the assumption that the quality assurance process software undergoes before it's released somehow insures there aren't vulnerabilities and insures proper functionality. If that were the case, then commercial software wouldn't ever show up on Bugtraq and bugfixes wouldn't exist. We all know, however, this isn't the case. Once we understand that the beta process for commercial software neither insures security nor functionality the argument against open source applications in a large enterprise pretty much loses steam.

This entire argument additionally assumes that all open source software is beta software and does not go through a quality assurance process. This is an assumption that does not hold true with snort. As you know, snort has a very large user base and in having such has a large quality assurance organization testing every beta build before it's released.

Large companies often feel like they must turn to business partners whom they have an established relationship with for every product regardless of the quality of the product the partner provides. Simply because a business partner provides an SLA on a sub-par product does not mean the product will function as promised. When dealing with the security of a large enterprise, I'll take functionality first and promises from

SecurityFocus IDS: Re: IDS recommendations

vendors second.

I'll leave the host based ID argument alone for the moment because I feel it is outside the scope of this thread. However I will add that snort is most definately fit for large enterprise environments.

–Jeff

--

<http://jeff.wwti.com> (pgp key available)

"Common sense is the collection of prejudices acquired by age eighteen."

– Albert Einstein

- ***Previous message:*** Chris Eidem: "RE: IDS on Switched Networks"
- ***In reply to:*** Nate.Duzenberry@mortgage.wellsFargo.COM: "RE: IDS recommendations"
- ***Next in thread:*** Talisker: "Re: IDS recommendations"
- ***Next in thread:*** Chris Eidem: "RE: IDS recommendations"
- ***Reply:*** Talisker: "Re: IDS recommendations"
- ***Messages sorted by:*** [date] [thread] [subject] [author] [attachment]