

Re: Cannot open log for source {0} -- again

Source:

<http://www.derkeiler.com/NewsGroups/microsoft.public.dotnet.framework.aspnet.security/2005-04/0099.html>

From: Joseph MCAD (*anonymous_at_microsoft.discussions.com*)

Date: 04/07/05

Date: Thu, 7 Apr 2005 08:41:13 -0700

April 6, 2005

I haven't read all of this thread, but check the Web Application Cannot Access Event Log 4/4/2005 in microsoft.public.dotnet.security. I have already helped some one out there and it appears that everything is solved!

:--)

Joseph MCAD

"Craig Wagner" <craig_d_wagner@hotmail.com> wrote in message news:ukfa51dvep3bfd5cmfrk0547rvo3p9j1ii@4ax.com...

> "Nicole Calinoiu" <calinoiu REMOVETHIS AT gmail DOT com> wrote:

>

>>Sure, but web applications are a poor candidate for writing to the
>>application log for security reasons. Even if you're only logging
>>exceptions, a malicious user of the web application could cause your event
>>log to either fill or dump (clearing old entries to make place for new
>>ones)

>>simply by forcing exceptions, thereby exposing you to either a denial of
>>service attack (via log filling) or hiding of clues to other activities
>>(via

>>log dumping). For this reason, you would be better off writing to a
>>custom

>>log rather than the default application log. At least with this approach,
>>abuse of your web application won't affect the logging activities of local
>>applications. You should also select the fill/dump behaviour of your
>>custom

>>log carefully since you'll still be subject to the DOS vs overwrite issue,
>>even if it's restricted to only the single application.

>

> So when you said that writing to the event log from a web app wasn't a
> good

> idea, what you really meant was writing to the default application event
> log

> wasn't a good idea.

>

> Now what if there are no other apps running on the server? This is the

microsoft.public.dotnet.framework.aspnet.security: Re: Cannot open log for source {0} -- again

> only
> application.
>
>>That's fine if only your application (and/or others that also require the
>>same logging permissions) are run under this account. However,
>>applications
>>that cannot be trusted to write to the log should not run under an account
>>with logging permissions.
>
> Agreed. But every application running on the server is an in-house
> developed
> application, so they can all be trusted to write to the log and, in fact,
> we
> want them logging a subset of their activities and unhandled exceptions
> should
> they occur for troubleshooting and debugging purposes.
>
> We could mitigate some of the potential for abuse by having each
> application
> (assuming there was more than one at some point) write to a different
> custom
> event log I suppose. But it seems to me the bottom line from this thread
> is that
> we just keep moving or mitigating the potential for trouble.
>
> And I purposely used the term "potential" twice, because we're a very
> targeted
> site used by our clients only. Yes, someone could stumble on it and try to
> be a
> dick and bring it down, but we're hardly worth the effort. We've had no
> incidents in the past five years. Sure, ignorance is no defense, and it
> isn't
> the only thing we do to take steps to protect ourselves, but we also need
> to
> weigh potential against complexity.
>
> --
> Craig Wagner, craig.wagner(at)comcast.net
> Portland, OR
>
> "Don't ban high-performance vehicles, ban low-performance drivers!"

Re: Cannot open log for source {0} -- again