

Re: EXEC master..xp_cmdshell Prevention

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2002-10/3163.html>

From: Beth Breidenbach (beth.breidenbach@getronics.com)

Date: 10/24/02

From: "Beth Breidenbach" <beth.breidenbach@getronics.com>

Date: Thu, 24 Oct 2002 08:34:46 -0700

Well, the quote-doubling helps, but I hope they can guarantee that none of their parameters are numeric (and thus not requiring any quote marks at all for me to hijack). Otherwise your box/network is still at risk. :-(

If you're having to host an 'other-developed' app the recommendation to secure your service's privileges becomes even more important. Feel free to drop me an email if you want to discuss further.

"Robert Robbins" <rrobbins@kolbnetworks.com> wrote in message news:urdaqrndpd7096@corp.supernews.com...

> Hello Beth,

>

> I found that my web application did use a connection string in a file
> other than the global.asa. I did not develop this application so creating
> stored procedures for every SQL statement would be impractical. They just
> released a critical update for SQL Injection vulnerabilities but it is
just

> a function that replaces single quotes with two single quotes (not to
> mention it introduces unrelated bugs). I have created a new login account
> for applications and an application role for my database. Creating
> application roles is not well documented so I will have to experiment with
> this to ensure I got it right.

>

> Robert Robbins

> Kolb Net Works

>

>

> "Beth Breidenbach" <bbreidenbach@mindspring.com> wrote in message
> news:ehyEhoheCHA.1572@tkmsftngp08...

> > Robert,

> >

> > I take it you're using string concatenation to build your sql
statements.

> I

> > strongly recommend against this as it opens up a whole slew of

> > vulnerabilities, including the xp_cmdshell one you're asking about. For

microsoft.public.sqlserver.security: Re: EXEC master..xp_cmdshell Prevention

&