

Re: IIS / Web Services Security threats

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.webservices/2005-04/msg00133.htm>

- *From:* Rafal Gwizdala <gwrafal@xxxxxxxxxxxxxxxx>
 - *Date:* Mon, 11 Apr 2005 22:43:07 +0200
-

Magdelin wrote:

Hi Henk,

Thanks for your response. You will be surprised to know, due to a recent virus attack on the perimeter network, the common ports have been closed too. My company is pretty new to .NET or basically to web based applications. Only Mainframe and desktop applications were developed in the past decade.

I also develop Java applications which runs on weblogic server. You will not believe the weblogic designated ports are open in firewall. Since, the entire world knows about port 80 and 443, I thought opening a specific port with IP Sec configuration may make the network little secure. Although, I know you can find out which ports are open by writing a small program.

Thanks once again,
Magdelin

"Henk Verhoeven" wrote:

Magdelin,

Are there any reasons why you do want to open alternate ports, usually this will freak out any security "expert".

If you run it on the same ports that is open right now (I assume of course), like HTTP, HTTPS, FTP

Re: IIS / Web Services Security threats

then you can use the same argument they use, that IIS is exposed and very bad people going to infiltrate.

Use the existing ports, make sure your web services communication is secure, tokens, encryption or ssl and you should be fine.

henk

"Magdelin" <magdelinsuja@xxxxxxxxxxxxxxxxxxxxxx> wrote in message news:CBAB91C3-58F6-490C-A080-98998478B626@xxxxxxxxxxxxxxxxxxxxxx

Hi,

My security team thinks allowing communication between the two IIS instances leads to severe security risks. Basically, we want to put our presentation tier on the perimeter network and the business tier inside the fire wall or internal network. The biz tier will be developed and deployed as web services on IIS.

I know microsoft recommends this architecture but I am not able to convince my security team. They say IIS is vulnerable to viruses and worms even though the communication between the web and app servers are secure with a firewall/SSL/IPSec. Even though we will open specific ports for accessing the web services, is it true that IIS is not a secure environment to access it from the perimeter network.

If my security team is true, I wonder what would be the alternative to IIS. If they are not, how should we protect our network while allowing web service

Re: IIS / Web Services Security threats

to run on IIS.

I have read all security related recommendations published by Microsoft but no luck with my security team yet. Esp. the entire document from patterns & practices:
Improving Web Application Security - Threats and Countermeasures

How are secure .NET enterprise applications developed and hosted in IIS?
Are there any companies out there which uses this MS recommended architecture and yet have a secure network?

Thanks,
Magdelin

Hello,

If you want to experiment with .Net and web services you don't have too many alternatives to IIS (at least I don't know any). But I have been using IIS + .Net for quite a long time and didn't find any unusual security problems (every software has some security problems that need to and are constantly patched by their authors, this also applies to IIS). Your case is quite typical: a public web server (accessible from the Internet, let's call it 'frontend') communicating with application server in the intranet. In case of .Net the application server is very often hosted in another IIS and is accessed by the frontend server using .Net Remoting. The communication with the application server is very often based on HTTP + SOAP - the frontend server makes HTTP calls to application server, and the application server listens on single port - 80 for example. The application server does not initiate any connections to the frontend server - all connections are initiated by frontend and go to application server.

This configuration is very simple for network administrators to maintain, and very easy to keep secure - using firewalls, ipsec or other secure protocols. There is only one application server port that needs to be made accessible to the frontend server, so you don't have to open any additional 'holes' in your intranet firewall.

And when it comes to the frontend server security - well, your security team should know how to secure public HTTP server - IIS is no different

Re: IIS / Web Services Security threats

in this aspect than any other server. It is important that in the architecture described above the frontend server is just what its name says - just a frontend, does not contain business logic and data. All important information is managed and kept by the application server.

So, summing up, there is no security problem introduced by the fact that two IIS-es communicate. This is the common case (the case described above), and I think that it is even more secure than other possible solutions with .Net web applications.

Best Regards
Rafal Gwizdala