

(Asp.Net Full Trust Vulnerabilities) RE: Apache VS IIS Security model question

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2004-09/0248.html>

From: Dinis Cruz (dinis_at_ddplus.net)

Date: 09/15/04

To: <ken@adopenstatic.com>, <webappsec@securityfocus.com>, <pen-test@securityfocus.com>, "'Full-d
Date: Tue, 14 Sep 2004 23:08:30 +0100

If the code is running with full trust it can call `RevertToSelf()` and change the current Asp.Net (Thread) Identity into the Process' Identity (which belongs to the IIS_WPG).

Once this is done:

1) You can probably already bypass several NTFS restrictions and see other website's data (and other sensitive information usually left on the server)

2) You can read (from the Metabase) other website's Anonymous and Application Pool Account details (Username and Password), use that information to impersonate those users (which you can with Full Trust) and access other website's data

3) If other websites share the same application pool, you can search the current `w3wp` process for their security tokens, use those tokens to impersonate those users (no need to know their password) and access website's data

4) You can upload to the server an exploit and execute it. With full trust it is almost impossible to stop the upload and execution of a malicious .EXE. The only defence could be if the Anti-Virus installed on the server is able to detect the Malware (although this limitation could be easily bypassed by any half-decent malicious attacker with access to the exploit's source code)

5) etc, etc, etc..... There any many more attack vectors, but these should be enough to make my point

Note that even if the attacker is only able to gain read access to another website's data, most likely he/she will be able to retrieve the Database Connection String and gain FULL access to that website's database.

If this is news for you (i.e. how dangerous Full Trust Asp.Net can be), then I would recommend that you take a good look at the work I have done over the

SecurityFocus Penetration: (Asp.Net Full Trust Vulnerabilities) RE: Apache VS IIS Security model question

last year at OWASP (Open Web Application Security Project), namely Open Source tools: ANSA (Asp.Net Security Analyser) and SAM'SHE (Security Analyser for Microsoft's Shared Hosting Environment).

Some links:

– OWASP .NET section: <http://www.owasp.org/software/dotnet.html>

– Post with Links to some of my online posts (Security issues with Asp.Net in Shared Hosting Environments, OWASP .Net tools and OWASP AppSec Presentation):

http://sourceforge.net/mailarchive/forum.php?thread_id=5203278&forum_id=24754

– presentation that I did last June at the OWASP AppSec NYC 2004 conference entitled "Full Trust Asp.Net (in)Security / Secure Asp.Net Web Application Development":

– http://prdownloads.sourceforge.net/owasp/AppSec2004-Dinis_Cruz-Full_Trust_Asp.Net_Security_Issues.ppt?download (main PPT)

– http://prdownloads.sourceforge.net/owasp/AppSec2004-Dinis_Cruz-Full_Trust_Videos.zip?download (the support videos: "ANBS – SamShe.avi", "ANBS – XML database and Metabase explorer.avi", "IIS Security Token Vulnerability.avi", "ANSA – Run tests individually.avi", "ANSA – Security Analyser.avi")

Best Regards

Dinis Cruz
.Net Security Consultant
DDPlus

> -----Original Message-----

> From: Ken Schaefer [mailto:ken@adopenstatic.com]

> Sent: 14 September 2004 03:10

> To: webappsec@securityfocus.com; pen-test@securityfocus.com

> Subject: RE: Apache VS IIS Security model question

>

> I'm pretty sure that Mike is talking about NTFS permissions (and Windows users and groups). Can you point us to how ASP.NET code running as fully trusted gets around that?

>

> Cheers

> Ken

>

> ----- Original Message -----

>> From: "Dinis Cruz" <dinis@ddplus.net>

>> Subject: RE: Apache VS IIS Security model question

>>

>> Please note that these security settings will only be relevant (in IIS)

> in a

(Asp.Net Full Trust Vulnerabilities) RE: Apache VS IIS Security model question

SecurityFocus Penetration: (Asp.Net Full Trust Vulnerabilities) RE: Apache VS IIS Security model question

> > *Partially Trusted Website (i.e. the Asp.Net code is NOT running with
> Full
> Trust).*
> >
> > *If the code is running with Full Trust, then most likely those security
> > permissions will be easily bypassed.*
> >
> > *Dinis Cruz
> > .Net Security Consultant
> > DDPlus*
> >
> > > -----Original Message-----
> > > *From: mthompson [mailto:mthompson@brinkster.com]
> > > Sent: 11 September 2004 01:56
> > > To: webappsec@securityfocus.com; pen-test@securityfocus.com
> > > Subject: Apache VS IIS Security model question*
> > >
> > > *Hello,*
> > >
> > > *I am doing research and I am stuck.*
> > >
> > > *Pitch: In IIS there is the ability to set permissions on a per website
> > > basis. In other words the ability to limit access to files and
> > > directories based on the users credentials that the website is running
> > > under. Additionally, you would in turn add this user to a group and
> > > apply group permissions to an object that needed to be accessed by
> > > more
> > > than one site.*
> > >
> > > *Question: Is there a similar security model for apache that would
> > > allow
> > > credentials from a user to run a virtual website and access files only
> > > for a specific virtual site.*
> > >
> > > *Also, does any one have a diagram of the apache process?*
> > >
> > > *Thanks,*
> > >
> > > *Mike*
> > >
>
>
>
>

> -----
> *Ethical Hacking at the InfoSec Institute. All of our class sizes are
> guaranteed to be 12 students or less to facilitate one-on-one interaction
> with one of our expert instructors. Check out our Advanced Hacking course,
> learn to write exploits and attack security infrastructure. Attend a
> course*

- > *taught by an expert instructor with years of in-the-field pen testing*
- > *experience in our state of the art hacking lab. Master the skills of an*
- > *Ethical Hacker to better assess the security of your organization.*
- >
- > http://www.infosecinstitute.com/courses/ethical_hacking_training.html
- >

> -----
>

Ethical Hacking at the InfoSec Institute. All of our class sizes are guaranteed to be 12 students or less to facilitate one-on-one interaction with one of our expert instructors. Check out our Advanced Hacking course, learn to write exploits and attack security infrastructure. Attend a course taught by an expert instructor with years of in-the-field pen testing experience in our state of the art hacking lab. Master the skills of an Ethical Hacker to better assess the security of your organization.

http://www.infosecinstitute.com/courses/ethical_hacking_training.html
