

RE: IIS6 Security and other web servers

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2005-01/0400.html>

From: Roger A. Grimes (*roger_at_banneretcs.com*)

Date: 01/28/05

Date: Thu, 27 Jan 2005 23:12:06 -0500

To: "Randy Williams" <randyw@techsource.com>, <security-basics@securityfocus.com>

Randy,

Any Internet-facing server without intervening layers of defense sounds risky to me...no matter who is the vendor.

However, my www.hackiis.com contest coming in April will test just the point you made...how secure is it by itself.

-----Original Message-----

From: Randy Williams [mailto:randyw@techsource.com]

Sent: Thursday, January 27, 2005 11:36 AM

To: security-basics@securityfocus.com

Subject: Re: IIS6 Security and other web servers

Greetings All,

I'd like to ask for some clarification here. I know that Ebay, Anandtech, et al. run on a purely Windows architecture (for the ease of programming in .Net from what the folks at Anandtech are saying) for their web-services and that works well for them.

However, I know of no Windows architecture that is exposed directly to the Internet. Every vendor/consultant/Admin I have ever met is saying that in order for Windows to be secure it must be protected by layers of protection (hardened router, hardware firewall, etc).

On the other hand, I know of a number of LAMP-type servers that are exposed directly to the Internet with no intervening layers.

Am I to take the statement that "IIS6 is a very secure platform" to mean that IIS6 is only secure after it has been hardened from its insecure default installation and protected by layered security that prevents direct access to the Internet".

I may well be wrong here, so please feel free to correct me if I'm out on a limb.

SecurityFocus BASICS: RE: IIS6 Security and other web servers

Thank you,

RandyW

Roger A. Grimes wrote:

>IIS6 is a very secure platform. Some of the largest and most
>Internet-exposed companies in the world run it. Ebay runs it. Like any
>web server, you must follow basic guidelines and keep your patches
>up-to-date, but that is any product.
>
>If you have mostly Windows experience, it certainly isn't a poor
choice.
>Anyone saying otherwise is just going on inaccurate or old data, or
>just letting their personal preferences get involved. I use both IIS
>and Apache, and both are secure when implemented as recommended. I'm a
>Windows guy, though, so configuring security and other things is easier

>for me in IIS (click, click, click) than in Apache (find text file to
>edit...).
>
>In fact, Windows IT Pro mag and I are sponsoring a Hack IIS contest in
>a few months with prizes.
>
>Roger
>
>*****
>*
>***
>*Roger A. Grimes, Banneret Computer Security, Computer Security
>Consultant *CPA, CISSP, MCSE: Security (NT/2000/2003/MVP), CNE (3/4),
>CEH, CHFI
>*email: roger@banneretcs.com
>*cell: 757-615-3355
>*Author of Malicious Mobile Code: Virus Protection for Windows by
>O'Reilly *<http://www.oreilly.com/catalog/malmobcode>
>*Author of Honeypots for Windows (Apress)
>*<http://www.apress.com/book/bookDisplay.html?bID=281>
>*****
>*
>****
>
>
>
>-----Original Message-----
>From: Rivera Alonso, David [mailto:drivera@iberdrola.es]
>Sent: Tuesday, January 25, 2005 9:52 AM
>To: security-basics@securityfocus.com
>Subject: IIS6 Security and other web servers
>
>

RE: IIS6 Security and other web servers

SecurityFocus BASICS: RE: IIS6 Security and other web servers

>Dear friends,
>
>I just want to throw a little question to know your opinion.
>I was discussing yesterday with a friend about the quality of IIS6 from

>a Security point of view.
>He immediately said it's a bad choice, as previous Microsoft web
>servers.
>I've read a few papers and I have this opinion: as it's been redesigned

>from the ground (with all the previous failures in mind), with the
>security perspective, with every little service and option disabled by
>default, and so on, I told him that now, in my opinion, IIS6 is a good
>choice.
>He loves GNU, Linux, and, logically, he thinks Apache is the king in
>security.
>Just because I felt curious, I went into www.securityfocus.com to check

>the latest vulnerability advisories, for Apache and IIS6. Incredible,
>Apache wins, it has many more (not to talk about the many releases
>since version 2.0)! In fact, I just found one alert about IIS6.
>
>What do you experts think?
>Of course, I know IIS was very dangerous before version 6.
>But, maybe an IIS6 in a well configured, patched and securized Windows
>2003 machine is at last a good choice to house Web Applications?
>Or maybe it's too soon, there are few installed, and maybe in the
>future it'll have as many holes as the predecessors?
>
>What do you think?
>
>best regards from Spain,
>
>DAVID
>
>
>
>
>=====

>Este mensaje se dirige exclusivamente a su destinatario.
>Puede contener informacion confidencial sometida a secreto profesional
>o cuya divulgacion este prohibida, en virtud de la legislacion vigente.

>No esta permitida su divulgacion, copia o distribucion a terceros sin
>la autorizacion previa y por escrito de Iberdrola.
>Si ha recibido este mensaje por error, le rogamos nos lo comuniquen
>inmediatamente por esta misma via y proceda a su destruccion.
>
>This e-mail is intended exclusively for the individual or entity to
>which it is addressed and may contain confidential or legally
>privileged information, which may not be disclosed under current

SecurityFocus BASICS: RE: IIS6 Security and other web servers

>legislation. Any form of disclosure, copying or distribution of this
>e-mail is strictly prohibited, save with written authorisation from
Iberdrola.

>If you have received this message in error, please notify the sender
>immediately by e-mail and delete all copies of the message.

>=====

>
>
>
>