IIS Security Overview

In recent years, IIS has gained quite a reputation for itself. Unfortunately, a big part of that reputation is for a lack of security. IIS 6 purports to solve many of IIS's security problems, but will it really? To help answer that question, we've compiled a list of the many reasons IIS is considered insecure in the first place. Use this list to place IIS's reputation into a practical context, and think about what IIS 6 is doing to address these concerns:

- Since Windows 2000, IIS has been installed by default in a fully functional mode. That means many servers not even being used as Web servers include IIS, making them vulnerable to any security holes in IIS. Administrators who religiously patched their Web servers with security updates often forgot about the non-Web servers that were running IIS, leaving those servers open to attack. Windows Server 2003 addresses this problem by not installing IIS by default, installing it in a locked-down condition when it is installed, and removing accidentally installed copies of IIS when upgrading Windows 2000.
- Several highly exploited security holes in IIS left it open to attacks such as Red Alert, which propagated from one IIS machine to the next on a network. IIS 6 helps to address this issue by locking down many of the features that enable this type of attack by default. However, if an administrator enables advanced features—such as dynamic Web pages—then the server will still be open to any security flaws contained in the IIS code.
- IIS is free for Windows servers, making it a popular choice. Any popular Web server is going to be the target of attacks. In addition, Microsoft makes IIS, making any IIS server a potential target for the legions of Microsoft-haters out there who feel they need to prove that Microsoft can't produce a secure Web server. IIS 6 won't fix this problem, per se; Microsoft simply needs to produce a bulletproof product to put these types of attacks behind them. Unfortunately, Microsoft has not yet demonstrated its ability to produce a bulletproof product. Its early-2002 "security code review," which lasted for two months, allegedly squashed thousands of security-related bugs, but the actual security and stability of IIS 6 remains to be seen.
- Administrators often deploy IIS without being fully cognizant of the security risks involved. IIS 6 helps defray this problem by using a pretty basic, locked-down default configuration. However, an administrator with a little bit of knowledge—enough to turn on IIS's advanced features, say, without taking proper precautions—will always be more dangerous than an experienced administrator who knows the risks.

All in all, IIS 6 is likely to cause fewer security problems out of the box, simply because it won't be on every Windows Server 2003 box in existence. Hopefully, administrators will refrain from deploying IIS until they're familiar with the risks and the necessary precautions. And hopefully Microsoft's Secure Computing initiative will prove to be more than just lip service paid to a popular cause. In the end, we probably won't know how secure IIS 6 is until IIS 7 is ready to ship because subtle security flaws can often take a long time to surface. IIS 6 should, however, show us whether Microsoft is on the right track to producing a more secure and stable Web server product.