

Achilles Heel of Your Information Security Infrastructure

By Boris Loza, PhD, CISSP

Microsoft IIS (Internet Information Services) is one of the most widely used web servers internally (on the Intranet) and externally (on the Internet). Unfortunately, plagued by bugs and design vulnerabilities since its introduction, it could pose a significant security risk to your network if it is misconfigured and un-patched. Configuring, patching and monitoring of all IIS servers is essential to keeping your “security gates” shut. That said, you may not be aware of all web-servers in your organization. It is critical to discover them before a worm or virus does, or they may become the Achilles heel of your security defense.

Web servers are tempting targets for internal and external hackers

It is part of the software engineering paradigm that upon completion of a piece of software, we expect the code to contain bugs. We also expect the design to contain security flaws.

Applications that allow remote access pose twice the security risk as application that don't, because vulnerabilities can be used to compromise the network. Web servers, whether they are facing the Internet or not, are the piece de resistance for internal and external hackers.

Patching them is easy – if you can find them

People concerned with information security are very serious about patching all Microsoft IIS web servers as soon as any security patch is announced, being all too aware of the many Internet worms and viruses exploiting IIS bugs and design vulnerabilities. Yet non-legitimate IIS installations abound in most organizations and are often a surprise to the group responsible for IIS support.

Microsoft IIS comes free with any Windows 2000/XP server distribution. Users with local Administrator privileges can easily install IIS (and any other non-legitimate applications) on their workstations. In our experience, a periodic network scan turns up non-legitimate IIS installations by people who do not appreciate the risk they pose. One user explained to us that it was more convenient for him to test “some stuff” directly on his workstation instead of going to the lab. Another user confessed that she wanted to learn IIS in order to become a web server administrator. These are “fresh” installations, meaning no security patches have been applied and no special security set up implemented.

Undiscovered installations pose serious security risks

If you are unaware of all IIS web servers on your network, then you do not patch them, do not configure them properly and do not monitor them. They present a clear threat to the company's security infrastructure. For example, the one of the mostly destructing Internet worm/virus called Nimda [*CERT CA-2001-26*] looked for backdoors left by previous the IIS worms Code Red II

[CERT IN-2001-09] and Sadmin/IIS [CERT CA-2001-11]. It also attempted to exploit various IIS Directory Traversal vulnerabilities [CERT VU#111677 and CERT CA-2001-12]. Multiple vulnerabilities in Microsoft IIS are reported by CERT [CA-2002-09] at www.cert.org/advisories/CA-2002-09.html.

It's cheaper to find them than to ignore them

The cost of such vulnerabilities can be devastating. McAfee antiviral company states *"Based on estimates of more than two million machines being infected with the Nimda worm worldwide, we estimate the economic impact of the Nimda worm to be \$530,650,000,"* and *"clean-up costs alone would be much greater, taking the economic impact figure to well over \$1.9 billion and weeks to achieve."*

As timely patching all IIS servers becomes a more and more critical task for protecting your networks, you need to keep track of all existing IIS (whether installed by developers or/and curious users). In organizations with thousands of machines, it is a hefty task to keep track of all legitimate IIS web servers, never mind those installed without the explicit approval. Information security personnel must work hard to discover, assess, patch and properly secure all web servers found on the network.

Steps to find and patch your Achilles heel

The following steps may help you to deal with this situation.

- Have your Information Security Officer (ISO) establish and maintain a list of legitimate IIS web servers.
- Register all existing IIS web servers, providing the following information:
 - Business owner of the IIS
 - Business needs
 - IIS administrator (Name, business, home & cell phones numbers, pager, administrator's backup)
 - OS administrator (Name, business, home & cell phones numbers, pager, administrator's backup)
- Have the ISO review requests to install additional IIS web servers.
- Clearly establish the groups responsible for installing and supporting web servers. Allow only these groups to install IIS.
- Create, publish and propagate an IIS information security policy prohibiting non-legitimate IIS installations.
- Periodically use network-scanning tools to verify compliance with this policy.
- With your list of legitimate IIS web servers as your guide, identify non-legitimate IIS installations and immediately remove them from the network.
- Revoke local Administrator privileges for users who don't need them. Keep track of all users with local Administrator privileges (including business purposes of such privilege).
- Come up with alternate solution for projects that require web server usage (use Apache, Netscape, Tomcat, etc...).
- If applicable, reduce the number of already existing IIS installations.

Conclusion

Although discovering, reviewing and registering all existing and new IIS web servers can be a time-consuming and seemingly thankless task, it may pay off handsomely in the long term.