

SecureIIS Web Server Protection

INTEGRATED MULTI-LAYERED WINDOWS SERVER PROTECTION

SecureIIS prevents potentially damaging network traffic from penetrating your servers and compromising your web based applications.

Vulnerabilities in software applications are responsible for the vast majority of network security breaches and data loss. Specifically, web server applications like Microsoft's IIS are consistently targeted because of the ease of application deployment and potential flaws inherent with coding and configuration mistakes. Because web servers often provide a portal to the internal network, they require a more formidable and customized level of protection above and beyond what network firewalls or intrusion detection systems can provide. SecureIIS™ operates within IIS to actively inspect all incoming requests at each stage of data processing. In this way, SecureIIS prevents potentially damaging network traffic, whether encrypted or unencrypted from penetrating your servers and compromising your web based applications.

APPLICATION LAYER PROTECTION

eEye Digital Security pioneered the concept of application-layer protection, which has revolutionized proactive security. Unlike network-layer protection products, an application-layer solution works within the application that it is protecting. SecureIIS inspects requests as they come in from the network layer, as they are passed up to the kernel, and at every level of processing in between. If at any point SecureIIS detects a possible attack, it can take over and prevent unauthorized access and/or damage to the web server and host applications..

IIS ISAPI INTEGRATION

Retina discovers all the assets on a given network, including operating systems, SecureIIS was developed as an ISAPI filter, which allows for a tighter integration with the web server as compared to other application firewalls. SecureIIS monitors data as it is processed by IIS and can block a request at any point if it resembles one of many classes of attack patterns; including SQL injection and cross site scripting.

ZERO DAY PROTECTION

Unlike network firewalls and intrusion detection systems, SecureIIS does not rely upon a database of attack signatures that require regular updating. Instead, it uses multiple security filters to inspect web server traffic that could cause buffer overflows, parser evasions, directory traversal, or other attacks.

FAST FACTS

RUNS ON WINDOWS 2003
Server with IIS 6.0 and
Windows 2008 Server with IIS
7.0 (32-bit and 64-bit)

INTEGRATED TECHNOLOGY
does not affect server
performance

COMPATIBLE WITH COMMON
web-based applications
such as Flash, Cold Fusion,
FrontPage, Outlook Web
Access and more

PROTECTS AGAINST THE
following classes of attacks:
buffer overflow, parser
evasion, directory traversal,
general exploitation, high-
bit shellcode protection,
cross site scripting, and SQL
injection and more



eEye Digital Security®

SecureIIS protects against the following attacks:

SQL INJECTION

SecureIIS is designed to filter the most common commands and characters used in SQL injection attacks. This stops SQL injection attempts dead in their tracks and can be verified with Retina Web Security Scanner.

BUFFER OVERFLOW ATTACKS

SecureIIS checks the lengths of all client-supplied buffers. If the data is larger than the maximum size allowed, SecureIIS will drop the connection, thereby avoiding a buffer overflow.

PARSER EVASION ATTACKS AND HIGH-BIT SHELLCODE PROTECTION

Insecure string parsing can allow attackers to remotely execute commands on the machine running the web server. SecureIIS checks for various characters in a string that would allow an attacker to add on commands to a normal value. If these characters are found, SecureIIS will drop the connection. In addition, normal English-language web traffic does not contain high bit characters. SecureIIS will drop all requests containing high bit characters, which often signal a potential buffer overflow attack.

DIRECTORY TRAVERSAL ATTACKS

In certain situations, various characters and symbols can be used to break out of the web server's root directory and access files on the rest of the file system. SecureIIS checks for these characters and also blocks access to specific directories and can even alert when specified files or directories are accessed or modified or even deleted.

RFC COMPLIANCY AND OTHER ATTACKS

SecureIIS prevents attackers from manipulating the HTTP protocol in attempts to bypass security systems and exploit security holes. SecureIIS has additional checks in place to identify and drop requests that contain recognized patterns. Limitations are also placed on the size of uniform resource locators (URL/URI), HTTP variables, request methods, request header size and other HTTP-related content and payloads that try to use common commands like cmd.exe.

SYSTEM REQUIREMENTS

WINDOWS 2000 SERVER SP1+ WITH IIS 5.0

WINDOWS 2003 SERVER (32-BIT AND 64-BIT) WITH IIS 6.0

WINDOWS SERVER 2008 (32-BIT AND 64-BIT) WITH IIS 7.0

WINDOWS SERVER 2008 R2 (64-BIT) WITH IIS 7.5

INTEL PENTIUM II 400MHZ (OR COMPATIBLE)

256 MB OF RAM

AT LEAST 80MB OF FREE DISK SPACE

NETWORK INTERFACE CARD (NIC) WITH TCP/IP ENABLED

NOTE: IIS PROXY SERVER IS NOT SUPPORTED

NOTE: IIS 6.0 PERSONAL EDITION IS NOT SUPPORTED

About eEye Digital Security

Since 1998, eEye Digital Security has made vulnerability management simpler, less expensive, and more effective by providing the only unified vulnerability and compliance management solution that integrates assessment, mitigation, and protection into a complete offering. Consistently the first to uncover critical vulnerabilities and prevent their exploit, eEye leverages its world-renowned research and development to strategically secure customer assets. Thousands of mid-to-large size organizations, including some of the most complex IT environments in the world, rely on eEye solutions to protect against the latest known, unknown, and zero-day vulnerabilities.

See more at www.eeye.com

CONTACT INFORMATION

UNITED STATES
1.866.282.8276

NORTH AMERICA SALES
sales@eeye.com

GERMANY
+49 (0) 8031 2227 432

INTERNATIONAL SALES
sales.eu@eeye.com

UNITED KINGDOM
+44 (0) 20 8432 3490

www.eEye.com

111 THEORY, SUITE 250 | IRVINE, CALIFORNIA 92617