



SecureIIS™ Application Firewall

Proactive Web Server Security

Vulnerabilities in software applications are responsible for the majority of network security breaches. Specifically, web server applications like Microsoft IIS are consistently the most targeted for attack. Because web servers often provide a portal to your internal network, they require a more formidable and customized level of protection above and beyond what network firewalls or intrusion detection systems can provide.

Developed by eEye Digital Security as the first-ever IIS application firewall, 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.

True Application Layer Protection

eEye Digital Security introduced the concept of application-layer protection, which has revolutionized the concept of 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 level, as they are handed off at the kernel level, 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.

Integrated into the IIS Platform

SecureIIS was developed as an ISAPI, which allows it to integrate more tightly with the web server. 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. Because of eEye's extensive knowledge of the many ways in which IIS servers can be attacked, as well as the nature of an application firewall, even undiscovered vulnerabilities specific to IIS are secured.

Blocks Against Entire Classes of Known & Unknown Attacks

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 for such issues as buffer overflows, parser evasions, directory traversal and other attacks. Therefore, SecureIIS is able to block entire classes of attacks, including those attacks that have not yet been discovered.

Created by the Experts on IIS Vulnerability

Worldwide, eEye is recognized as one of the most trusted and respected sources dedicated to improving IIS security. In fact, eEye's research team is credited with the discovery of numerous high-severity IIS vulnerabilities that would have allowed an attacker to gain complete remote control over a susceptible server.

Fast Facts

- Runs on Windows NT 4, IIS 4 -or- Windows 2000, IIS 5
- Does not affect server performance
- Compatible with and protects all common web-based applications such as Flash, Cold Fusion, Front Page, Outlook Web Access and more
- Protects against the following classes of attacks: buffer overflow, parser evasion attacks, directory traversal attacks, general exploitation, high-bit shellcode protection, among other attacks

SecureIIS ensures that your IIS servers are continuously protected, avoiding the dangerous time lapse between when:

- A vulnerability is discovered
- Microsoft is alerted
- An appropriate patch is developed
- The patch is released
- Network administrators worldwide are notified
- Confirmation that the patch has no bugs or software conflicts
- Web servers are taken offline to prepare for deployment
- The patch is downloaded and installed



eEye® Digital Security



SecureIIS™ Application Firewall

Additional Features and Benefits

- **Central Policy Management**
Ability to manage settings for any number of machines from a single, central location.
- **Logging of all Blocked Requests**
The log provides detailed explanations as to why requests were denied. Accessible from the main interface.
- **Run-Time Switching**
Configurations can be modified without having to restart the web server, thus disrupting the active website.
- **Real-Time Statistic Charts**
Monitors activity in real time by providing graphs based on the class of attacks.
- **Non-Intrusive Protection**
Protection without affecting service levels on your web server. Improved performance when the server is under attack.
- **Third-Party Application Protection**
Stops attacks launched against any third-party web server applications or custom web-page scripts.
- **Protection Against SSL Encrypted Sessions**
Stops attacks on encrypted sessions based on the ability to analyze HTTPS sessions before and after SSL (Secure Socket Layer) encryption.
- **Flexible Export Capability**
The log can be exported in any number of different formats including tab delimited, text, Excel, SQL and more.
- **Compatible with Web-Based Applications**
Works with and protects all common web-based applications such as Flash, Cold Fusion, Front Page, Outlook Web Access.
- **File System Activity Monitoring**
SecureIIS can send alerts when such activities as file additions, deletions and modifications occur.
- **Global-Settings Adjustment**
Reconfigure the application globally across all sites on a server, on a per site basis or on a per virtual directory basis thru an intuitive point-and-click interface.

SecureIIS protects against the following attack types:

- **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**
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.
- **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.
- **General Exploitation**
By checking for common attacker "payloads" such as cmd.exe in the exploiting data, SecureIIS can prevent an attacker from gaining unauthorized access to your web server and its data.
- **High-Bit Shellcode Protection**
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.
- **RFC Compliancy**
SecureIIS prevents attackers from manipulating the HTTP protocol in attempts to bypass security systems and exploit security holes.
- **Other Attacks**
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.

System Requirements

- Windows NT 4.0, IIS 4.0 and Service Pack 6
or
- Windows 2000, IIS 5.0 and Service Pack 1 or greater

About eEye Digital Security

eEye Digital Security is a leading developer of advanced network security products that deliver unsurpassed levels of protection against malicious attacks and undetected vulnerabilities. A global company with offices in the US and throughout Europe, eEye helps protect the digital assets of major corporations and government entities in over 40 countries.

eEye Digital Security
www.eEye.com

U.S. Tel: 1.866.339.3732
N. America: 1.949.349.9062
Geneva: +41 22.787.2282
London: +44 (0)20.8233.2845
Madrid: +34 91.700.4430
Paris: +33 1.58.71.40.31



eEye® Digital Security

N. America: sales@eeye.com
International: sales.eu@eeye.com

VULNERABILITY IS OVER