



Using Palo Alto Networks to Protect Microsoft SharePoint Deployments

June 2009

Palo Alto Networks
232 East Java Dr.
Sunnyvale, CA 94089
Sales 866.207.0077
www.paloaltonetworks.com

Table of Contents

Introduction.....	3
Step 1: Identify SharePoint Components.....	4
Step 2: Isolate the Components (MS-SQL, IIS, SharePoint).....	5
Step 3: Apply User-based Policy Controls.....	5
Step 4: Protect SharePoint Environments From Threats.....	6
Palo Alto Networks Helps Protect SharePoint Environments.....	7
Appendix 1: Threats Detected in SharePoint Deployments.....	8

INTRODUCTION

Microsoft SharePoint is a browser-based collaboration tool that can be used to host web sites, termed SharePoint Portals, which in turn, can provide access to shared workspaces, documents and specialized applications such as wikis and blogs. SharePoint functionality is exposed as web parts, which are components that implement a certain function, such as a task list, or discussion pane. Web parts are presented as web pages that are then hosted in the SharePoint portal. SharePoint sites are actually ASP.NET applications, which are served using Microsoft IIS and use a Microsoft SQL Server database as data storage backend.

In terms of market awareness, SharePoint currently holds approximately 20% of the market placing it 3rd behind Oracle and IBM. Year over year growth however is a staggering 48% compared to 11% and 12% for the other two vendors. The Spring 2009 and Fall 2008 editions of the Palo Alto Networks Application Usage and Risk Report validates the popularity of SharePoint with the application being found in 86% of the enterprises (n=123) analyzed over a 12 month period.

SharePoint is available in two configurations: Windows SharePoint Services (WSS) and Microsoft Office SharePoint Server (MOSS).

- WSS is included for free as part of the Windows Server package. WSS is ideally suited for stand-alone deployments and provides templates to build team sites, document workspaces, blank sites, blogs, wikis, and meeting workspaces. WSS can integrate with Microsoft Office (Word, PowerPoint, Access, Excel, and Outlook). When documents or content changes, RSS feeds can notify users as needed.
- MOSS is a licensed software solution that is targeted at large, server farm deployments. MOSS offers all of the features included in WSS as well as business intelligence features that allow users to track key performance indicators and build BI dashboards into the collaboration or web site. Whereas WSS can display Office files, MOSS can stream the files, showing or hiding various parts.

Both SharePoint incarnations are three tiered architectures with IIS as the front-end, the web application as the mid-tier, and a back-end database, either an internal database (WSS) or MS-SQL (WSS and MOSS).

The risks that SharePoint deployments represent may appear to be limited because it is viewed as a business application that is supported (and secured) by IT. In reality, recent research [by Neil MacDonald at Gartner shows that as many as 30% of the SharePoint deployments are rogue](#). A rogue SharePoint deployment is similar to the rogue wireless deployments of years ago.

The risks that IT managers face when deploying SharePoint are both business and threat oriented. From a business perspective, IT needs to be able to enable the collaborative nature while maintaining compliance with regulatory and/or internal policies that dictate who has access to the applications and who may be able to post. From security perspective, there are two key elements to consider.

The first element is to make sure that the SharePoint components (IIS, MS-SQL, SharePoint) are protected from threats. IIS and MS-SQL are both highly visible targets for vulnerability exploits so appropriate security steps should be taken. The second element to account for is data loss from unauthorized access or targeted attacks focused on MS-SQL.

This document will discuss how Palo Alto Networks' next-generation firewall can be used to complement SharePoint deployment best practices in supported environments and mitigate business and security risks associated with rogue SharePoint deployments.

STEP 1: IDENTIFY SHAREPOINT COMPONENTS

The first area where Palo Alto Networks can help secure a SharePoint environment is to determine which of the SharePoint components are in use. Part of the challenge that SharePoint presents to IT departments is the fact that it looks like common web traffic (HTTP or HTTPS), making it more difficult for to delineate the SharePoint traffic from web traffic in order to apply appropriate security controls using today's existing port-based security tools.

Palo Alto Networks is the only firewall on the market that uses a patent-pending technology called App-ID™ to identify and control more than 800 applications, irrespective of port, protocol, SSL encryption or evasive tactic employed. The determination of the application identity by App-ID is done inline (not proxied) using four different techniques (decoders, decryption, signatures and heuristics) to determine the application identity which is then used as the basis for all policy decisions including appropriate usage, content inspection, logging and reporting.

Currently App-ID identifies and controls six different SharePoint elements including: SharePoint, SharePoint-admin, SharePoint-blog-posting, SharePoint-calendar, SharePoint-documents, SharePoint-wiki. With this knowledge of which components are in use, IT can make a more informed decision on how to protect SharePoint and the users. Of the SharePoint features currently identified, the Application Usage and Risk Report shows that SharePoint and SharePoint-admin were most commonly detected.

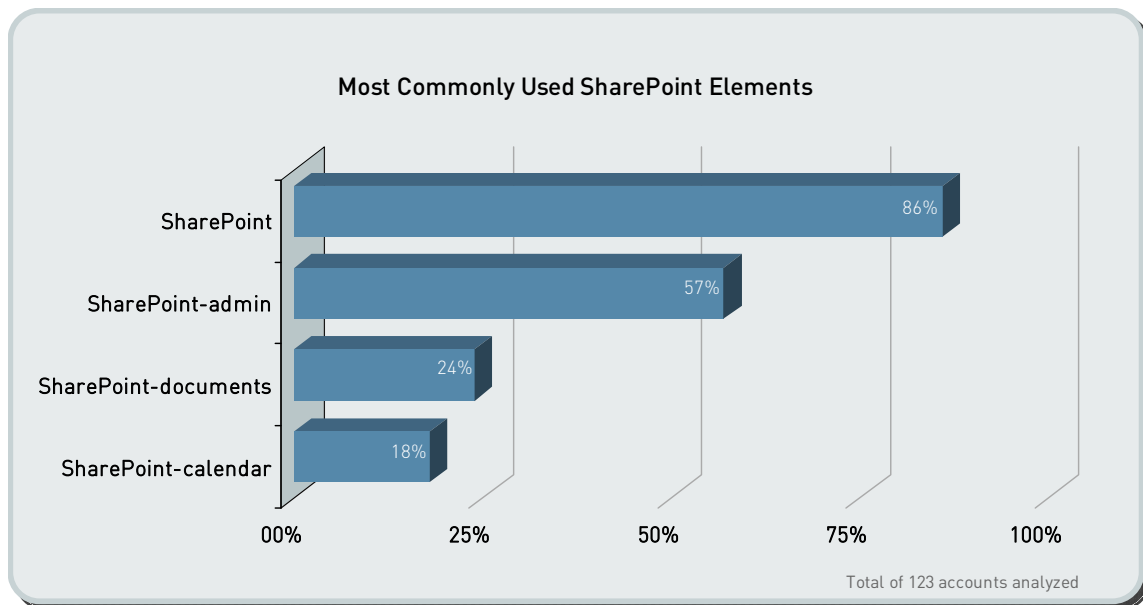


Figure 1: Most commonly discovered SharePoint functions used (CY2008).

Knowing the exact identity of the application means that instead of trying to implement security policies using broad-based terms such as IP address range, along with port and protocol, an IT manager can define a policy that enables or disables access to a specific application (e.g., SharePoint, SharePoint features and other supporting applications such as MS-SQL) for a specific set of users. Policies based on applications and users gives the security team far more granular control over network traffic, which results in an improved security posture. Accordingly, any successful or failed attempts at application access can be logged for forensics and auditing purposes.

In cases where SharePoint has been deployed by business units without the help, support or endorsement of corporate IT, Palo Alto Networks can help identify the location of the SharePoint server through the IP address and users via the user and group information within Active Directory. Depending upon the internal policy, the offending employees can be asked to stop, or a policy can be implemented that enables the use of SharePoint but from within the corporate security policies.

STEP 2: ISOLATE THE COMPONENTS (MS-SQL, IIS, SHAREPOINT)

The next step in protecting SharePoint environments is to isolate the different components (MS-SQL, IIS, and SharePoint server) by placing them in secure segments. Palo Alto Networks next-generation firewalls bring a unique combination of hardware and software related segmentation capabilities to customers who want to isolate key pieces of the network to improve their security posture. Every Palo Alto Networks firewall supports security zones, which is a logical container for physical interface(s), VLANs, a range of IP addresses or a combination thereof.

The most critical element to protect is the MS-SQL database application as it holds all the data that the SharePoint-based applications utilize. Using security zones as a means to isolate the MS-SQL database, the SharePoint application, and possibly the IIS application via a security policy can help protect against unauthorized access, stop the loss of corporate data and mitigate threats targeted at the specific application elements.

In terms of controlling application access, the key differentiator that Palo Alto Networks provides, over and above any other firewall on the market, is the ability to control the applications, users and content that can traverse each security zone. Once the network has been divided into distinct zones, security policies can be applied that control, at a very granular level, which applications, users and content are allowed in and out of the zone that contain the SharePoint application elements.

By default, SharePoint accesses the data held in the MS-SQL database through an IIS-based application using tcp/port 1433. If this port is unavailable, then udp/port 1434 is used. Note that SharePoint never accesses the data directly – it is done through the applications running on IIS.

Using a Palo Alto Networks next-generation firewall, an administrator can first establish a SharePoint zone and an MS-SQL zone. Policies can then be enabled for the SharePoint zone that dictates which specific users can access the application. Policies can also be enabled to dictate which applications can access the MS-SQL zone. Finally, the policy can dictate that the traffic is forced only over a specific port, such as tcp/port 1433, thereby locking down from access via other ports. This means that any other application that might hop ports or tunnel another application will be blocked from accessing the zone. Accordingly, any applications that are not within the policy that attempt to access SharePoint within the zone can be logged for forensics and auditing purposes.

STEP 3: APPLY USER-BASED POLICY CONTROLS

SharePoint itself has very granular administrative user controls that enables an administrator to determine who can use which feature. Palo Alto Networks can act as the perfect complement to the built-in SharePoint role-based administration by first determining the components in use, and then applying specific policies that tie users and groups from Active Directory to SharePoint use. Policies can be deployed that enable/disable use of key SharePoint functions (SharePoint, SharePoint-admin, SharePoint-blog-posting, SharePoint-calendar, SharePoint-documents, SharePoint-wiki) for users and groups within Active Directory.

Palo Alto Networks delivers this capability with User-ID, a technology that seamlessly integrates with Active Directory, enabling user- and group-based policy control, without requiring an agent on every desktop. User-ID helps address the challenges presented to IT by an increasingly mobile enterprise, where employees access the network from virtually anywhere around the world, internal wireless networks re-assign IP addresses as users move from zone to zone, and network users are not always company employees.

With User-ID, a policy can be created that marries the application (e.g., SharePoint, MS-SQL, etc) with the user and group identity (e.g., Marketing, Engineering, Finance, External Contractors) stored within Active Directory. The policy can be created to allow only inbound traffic from the users and in so doing, limit the security exposure. Alternatively a policy can be created that says do not allow any other users or groups to access the SharePoint (or MS-SQL zone) zone.

STEP 4: PROTECT SHAREPOINT ENVIRONMENTS FROM THREATS

Controlling application access addresses only a small part of the SharePoint security challenge. An equal or greater challenge is addressing the specific threats that are targeted at SharePoint environments. If SharePoint itself were the only element to protect, then the task would be relatively straightforward. However, SharePoint relies on IIS and in many cases, MS-SQL which means that the exposure to vulnerability exploits is significantly higher. An evaluation of the data collected for the two most recently produced Application Usage and Risk Reports (Spring 2009, Fall 2008) shows that there were 38 different critical, high and medium severity threats detected (185,537 instances) that targeted SQL, IIS, ASP.NET and SharePoint. (See Appendix 1 for a complete list).

Using the Palo Alto Networks next-generation firewall, an administrator can easily add a threat prevention profile to the policy that detects and blocks vulnerability exploits that target SharePoint and the supporting applications.

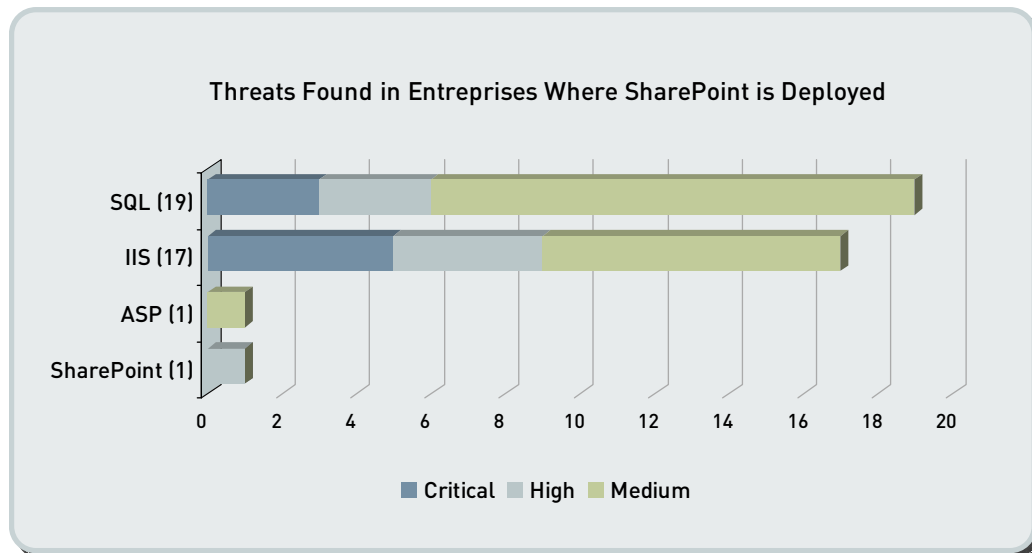


Figure 2: Critical, high and medium severity threats discovered in those companies where SharePoint was in use (CY2008).

In addition to the vulnerability exploit protection that Palo Alto Networks provides, a data filtering profile can be added that monitors SharePoint traffic for unauthorized transfer of confidential data. Files based on file type (as opposed to looking only at the file extension) and confidential data patterns (credit card and social security numbers) can be detected and blocked based on policy.

PALO ALTO NETWORKS HELPS PROTECT SHAREPOINT ENVIRONMENTS

Collaborative tools like SharePoint rely on efficient yet freeform information sharing to foster ideas, communicate efficiently and ultimately improve the bottom line. At face value, freeform communications flies in the face of security best practices (which may help explain the rogue deployments). With a Palo Alto Networks next-generation firewall, the IT department can enable the use of SharePoint while protecting users and the company from a wide range of data loss, compliance and security risks. Some examples of policies include:

- Isolate the SharePoint components (SharePoint, IIS, MS-SQL) using security-zones and apply policies that dictate which users can access those components.
- Implement policy control over SharePoint specific elements (SharePoint, SharePoint-admin, SharePoint-blog-posting, SharePoint-calendar, SharePoint-documents, SharePoint-wiki).
- Inspect traffic for a wide range of vulnerabilities and other forms of malware.
- Filter traffic for the unauthorized transfer of files and data (credit card numbers, social security numbers).

The visibility and control over applications, users and content that Palo Alto Networks allows the IT department to proactively support SharePoint deployments that foster collaboration while minimizing the business and security risks.

APPENDIX 1: THREATS DETECTED IN SHAREPOINT DEPLOYMENTS

Name	Instances	Severity	Category	Description	CVE
Microsoft IIS .printer ISAPI Extension Buffer Overflow	516	critical	code-execution	Microsoft Internet Information Server (IIS) version 5.0 installed on Microsoft Windows 2000 is prone to a buffer overflow while handling certain crafted HTTP requests. The vulnerability exists in the Internet Printing Protocol (IPP) ISAPI extension, which does not perform proper boundary checks while handling user input passed through HTTP requests. An attacker could exploit the vulnerability by passing a crafted request to the server, and cause remote code execution with the privileges of the server.	CVE-2001-0241
Microsoft IIS 5.0 WebDAV Remote Buffer Overflow Vulnerability	2979	critical	code-execution	WebDAV component of Microsoft Internet Information Services (IIS) Web server is prone to a buffer overflow vulnerability while parsing certain crafted HTTP requests. WebDAV stands for "Web-based Distributed Authoring and Versioning". WebDAV extensions are used by administrators to manage and edit Web content remotely and is enabled by default on IIS 5 installations. The vulnerability is due to the improper parsing of certain WebDav requests sent to the server, resulting in an exploitable overflow. An attacker could exploit the vulnerability by sending a crafted WebDav HTTP request. A successful exploit could lead to remote code execution with the privileges of the server.	CVE-2003-0109
Microsoft IIS Escaped Characters Decoding Command Execution Vulnerability	6912	critical	code-execution	Microsoft IIS is prone to a directory traversal vulnerability while parsing certain crafted http requests. The vulnerability is due to the lack of proper checks on url in the http request, leading to an exploitable arbitrary file request. An attacker could exploit the vulnerability by sending a crafted http request. A successful attack could lead to remote code execution with the privileges of the server	CVE-2001-0333
Microsoft IIS Executable File Parsing Vulnerability	435	critical	code-execution	Microsoft Internet Information Server is prone to a remote command execution vulnerability while parsing certain crafted http requests. The vulnerability is due to the lack of proper checks on the arguments to executable files , leading to an arbitrary command execution. An attacker could exploit the vulnerability by sending a crafted http request. A successful attack could lead to remote code execution with the privileges of the server.	CVE-2000-0886
Microsoft IIS WebDAV Request Source Code Disclosure	7	critical	code-execution	The vulnerability depends on resources specific to each website and knowledge about the path and name of scripts are required to be able to disclose their source code remotely. Moreover there is no patch available at this time and a difference behavior of the IIS server upon non-valid requests is not known. Therefore, remote deterministic zero-credentialed detection is not possible.	
Microsoft SQL Server Heap Overflow	3	critical	code-execution	Microsoft SQL Server is prone to a remote heap overflow vulnerability. A SQL request packet with the first byte set to 0x08, and followed by a long string before a colon character would overwrite the heap. A remote attacker could send a crafted packet which would corrupt critical heap structures to exploit the vulnerability. A successful attack may result in arbitrary code execution with SYSTEM privileges leading to a full compromise. Attack attempts may result in denial-of-service conditions as well.	CVE-2002-0649
Microsoft SQL Server Stack Overflow	976	critical	code-execution	Microsoft SQL Server is prone to a remote stack overflow vulnerability. A SQL request packet with the first byte set to 0x04, and followed by a long string would overflow the stack, as the server attempts to open a registry key with the data. A successful attack may result in arbitrary code execution with SYSTEM privileges leading to a full compromise. Attack attempts may result in denial-of-service conditions as well.	CVE-2002-0649
Microsoft SQL Server sp_replwritetovarbin Stored Procedure Buffer Overflow Vulnerability	5	critical	overflow	Microsoft SQL server is prone to a buffer overflow vulnerability while parsing certain crafted SQL function parameters. The vulnerability is due to the lack of proper checks on sp_replwritetovarbin in the SQL sentence request, leading to an exploitable buffer overflow. An attacker could exploit the vulnerability by sending a crafted SQL sentence request. A successful attack could lead to remote code execution with the privileges of the server.	CVE-2008-5416; CVE-2008-4270
CA BrightStor ARCserve Backup Agent For MSSQL Server Buffer Overflow	2	high	code-execution	BrightStor ARCserve Backup Agent for SQL Server 11.0 and earlier is prone to a buffer overflow vulnerability while handling long packets to TCP port 6070. The vulnerability is due to the improper handling of requests over 3168 bytes, leading to a stack overflow. An attacker could exploit the vulnerability by passing a long request to the backup system, causing remote code execution.	CVE-2005-1272
Microsoft IIS Extended Unicode Improper Canonicalization Directory Traversal	4313	high	code-execution	Microsoft Internet Information Server (IIS) versions 4.0 and 5.0 are prone to a directory traversal vulnerability while parsing certain URLs which use Unicode character sets. The vulnerability is due to improper canonicalization causing certain URI paths to be decoded to directory traversal paths. This could be exploited by an attacker to access arbitrary directories and files on the IIS server. A successful attack could be used to read, or write documents outside of the web root, and possibly to execute arbitrary commands. This vulnerability has commonly been exploited by CodeBlue worm.	CVE-2000-0884
Microsoft IIS HTR Request Parsing Buffer Overflow Vulnerability	53	high	code-execution	Microsoft Internet Information Server (IIS) version 4.0 before Service Pack 6 is prone to a buffer overflow while handling certain crafted HTTP requests. The vulnerability is due to the lack of boundary checks on the length of filenames with .htr, .idc and .stm extensions, processed as part of a HTTP URL. An attacker could exploit the vulnerability by passing a long filename in the URL,	CVE-1999-0874

Name	Instances	Severity	Category	Description	CVE
				overflowing the buffer. A successful exploit could lead to remote code execution, or lead to a denial of service condition on the server.	
Microsoft IIS nsiislog.dll ISAPI Extension Stack Overflow Vulnerability	3	high	code-execution	Microsoft Internet Information Server (IIS) is prone to a stack overflow vulnerability while parsing certain malformed HTTP requests. The vulnerability exists in the Internet Services Application Programming Interface (ISAPI) nsiislog.dll extension, while parsing large POST requests leading to a stack overflow. An attacker could exploit the vulnerability by sending a large malformed POST request, which could cause remote code execution.	CVE-2003-0349; CVE-2003-0227
Microsoft IIS Unicode Directory Traversal Vulnerability	8	high	code-execution	Microsoft Internet Information Server (IIS) versions 4.0 and 5.0 are prone to a directory traversal vulnerability while parsing certain URLs which use Unicode character sets. The vulnerability is due to improper canonicalization causing certain URI paths to be decoded to directory traversal paths. This could be exploited by an attacker to access arbitrary directories and files on the IIS server. A successful attack could be used to read, or write documents outside of the web root, and possibly to execute arbitrary commands. This vulnerability has commonly been exploited by CodeBlue worm.	CVE-2000-0884
Microsoft SQL Server sqldmo.dll ActiveX Buffer Overflow Vulnerability	51	high	code-execution	Microsoft SQL Server Distributed Management Objects component is prone to a stack overflow vulnerability. The vulnerability is present in the sqldmo.dll and is due to the lack of boundary checks on the length of arguments passed to certain methods of the DLL. Since these arguments are later copied to finite stack buffers, it could lead to an exploitable stack overflow condition. An attacker could exploit the vulnerability by crafting a webpage containing the control with a long argument to the method. A successful exploit could lead to remote code execution with the privileges of the current logged-in user.	
Microsoft Office Sharepoint Server Elevation of Privilege	50	high	info-leak	Microsoft Office SharePoint Server 2007 and Microsoft Office SharePoint Server 2007 Service Pack 1 is prone to an elevation of privilege vulnerability while parsing certain crafted http requests. The vulnerability could allow elevation of privilege if an attacker bypasses authentication by browsing to an administrative URL on a SharePoint site. A successful attack leading to elevation of privilege could result in denial of service or information disclosure.	CVE-2008-4032
phpnuke Search Module Query variable SQL Injection	355	high	sql-injection	phpNuke versions between 7.5 and 7.8 are prone to a SQL injection vulnerability in the search module. The vulnerability is due to the lack of sanitization of user-supplied input to the query parameter of the search module. An attacker could exploit the vulnerability by crafting a HTTP request and injecting SQL commands, in order to retrieve or modify sensitive database information.	CVE-2005-3792
Microsoft SQL Sever User Authentication Brute-force Attempt	40	medium		This event indicates that someone is doing a brute force attack and try to authenticated to the MSSQL database server.	
MySQL Authentication Brute-force Attempt	10	medium	brute-force	This event indicates that someone is doing a brute force attack and try to authenticated to the MySQL server.	
IIS WebDAV Denial of Service	3706	medium	dos	IIS 5.0 is prone to a denial of service vulnerability while parsing certain crafted HTTP requests. The vulnerability is due to the lack of proper checks on SEARCH request URI path length. An attacker could exploit the vulnerability by sending a crafted HTTP request. A successful attack could crash the server thus denying its services to other clients.	CVE-2003-0226
Microsoft ASP.NET Path Validation Security Bypass Vulnerability	7787	medium	info-leak	Microsoft ASP.NET is prone to an information disclosure vulnerability while parsing certain malformed HTTP requests. The vulnerability is due to a failure of the application to properly impose security restrictions while parsing URI paths containing certain characters. The vulnerability would allow an attacker to gain unauthorized access to certain restricted files or directories on the server.	CVE-2004-0847
Microsoft IIS Alternate Data Streams ASP Source Disclosure	397	medium	info-leak	Microsoft IIS web server is prone to an information disclosure vulnerability while handling certain crafted requests. The vulnerability is due to the improper handling of the various data streams that NTFS provides for a file, specifically alternate data streams. Thus by appending a string ":::SDATA" to a request URI, the contents of an ASP file could be retrieved instead of executing it. An attacker could exploit the vulnerability by sending a crafted HTTP request to the server, which could reveal sensitive information.	CVE-1999-0278
Microsoft IIS HTR Request Source Disclosure Vulnerability	512	medium	info-leak	Microsoft IIS web server is prone to a file source disclosure vulnerability while handling certain crafted requests. The vulnerability is due to the improper handling of URI requests with a "+.htr" appended. Such as request could lead to the disclosure of the source of the file requested in the URL. An attacker could exploit the vulnerability by sending a crafted HTTP request to the server, which could reveal sensitive information.	CVE-2000-0630
Microsoft IIS Sample Scripts Arbitrary File Disclosure Vulnerability	470	medium	info-leak	Microsoft IIS web server is prone to an arbitrary file disclosure vulnerability while handling certain crafted requests. The vulnerability is present in several sample ASP scripts such as show_code.asp, codebrws.asp, which allow viewing source of other sample files within same directory. However, since these scripts do not properly handle the source file requested, they allow retrieval of source of ASP files outside the directory using directory traversal paths. An attacker could exploit the vulnerability by sending a crafted HTTP request to the server, which could reveal sensitive information.	CVE-1999-0736; CVE-1999-0739

Name	Instances	Severity	Category	Description	CVE
Microsoft IIS Server Name Spoof Vulnerability	196	medium	info-leak	Microsoft IIS 5.1 and 6 are prone to an information leak vulnerability while parsing certain crafted HTTP requests. The vulnerability is because certain ASP scripts display source code when an error occurs if the SERVER_NAME variable is "localhost". In this case the script assumes the request is coming from the local web server and displays sensitive script code. Thus, an attacker could spoof the SERVER_NAME variable through crafted HTTP requests to retrieve sensitive information from the web server.	CVE-2005-2678
Microsoft IIS Translate F Header Source Disclosure Vulnerability	218	medium	info-leak	Microsoft IIS web server is prone to an information disclosure vulnerability while handling certain crafted requests. The vulnerability is present in the scripting engine and is due to the improper handling of requests sent with a special header "Translate: F". When this header is sent in a request with a slash appended to the URI path, the requested file source is returned by the server. An attacker could exploit the vulnerability by sending a crafted HTTP request to the server, which could	CVE-2000-0778
Microsoft IIS WebHits.DLL Directory Traversal Vulnerability	49	medium	info-leak	Microsoft IIS web server is prone to a directory traversal vulnerability while handling certain crafted requests. The vulnerability is present in WebHits.dll and is due to the improper handling of parameter value of the CiWebHitsFile parameter. A directory traversal value could be supplied to retrieve arbitrary files on the server. An attacker could exploit the vulnerability by sending a crafted HTTP request to the server, which could reveal sensitive information.	CVE-2000-0097
Microsoft IIS WebHits.DLL Source Disclosure Vulnerability	404	medium	info-leak	Microsoft IIS web server is prone to an information disclosure vulnerability while handling certain crafted requests. The vulnerability is present in WebHits.dll and is due to the improper handling of requests sent by appending a space at the end of CiWebHitsFile parameter value. This vulnerability could disclose ASP file source used as the parameter value. An attacker could exploit the vulnerability by sending a crafted HTTP request to the server, which could reveal sensitive information.	CVE-2000-0302
Microsoft SQL Server INSERT Statement Buffer Overflow Vulnerability	2	medium	overflow	There exists a buffer overflow vulnerability in Microsoft SQL Server. The vulnerability is specifically caused by insufficient data validation when processing parameters passed to CONVERT function in an SQL statement. A remote authenticated attacker can exploit this vulnerability to execute arbitrary code with System privileges on the target system.	CVE-2008-0086
Microsoft SQL Server INSERT Statement Buffer Overflow Vulnerability	9563	medium	overflow	There exists a buffer overflow in Microsoft SQL Server. The vulnerability is due to the way SQL Server improperly checks insert statements before processing them. A remote authenticated attacker can exploit this vulnerability by sending a specially crafted SQL to the target server, potentially causing arbitrary code injection and execution with the privileges of the affected process.	CVE-2008-0106
MSSQL Login failed for user 'sa' execution	1770	medium	overflow	This alert indicates that a suspicious command Login failed for user 'sa' is running on the MSSQL Server. The command when used, is highly likely to cause overflow, misused or other issues.	CVE-2000-1209
MSSQL raiserror execution	39832	medium	overflow	This alert indicates that a suspicious command raiserror is running on the MSSQL Server. The command when used, is highly likely to cause overflow, misused or other issues.	CVE-2001-0542
MSSQL sp_adduser execution	24	medium	overflow	This alert indicates that a suspicious command sp_adduser is running on the MSSQL Server. The command when used, is highly likely to cause overflow, misused or other issues.	
MSSQL sp_password execution	201	medium	overflow	This alert indicates that a suspicious command sp_password is running on the MSSQL Server. The command when used, is highly likely to cause overflow, misused or other issues.	
MSSQL sp_start_job execution	135	medium	overflow	This alert indicates that a suspicious command sp_start_job is running on the MSSQL Server. The command when used, is highly likely to cause overflow, misused or other issues.	
MSSQL xp_cmdshell execution	9707	medium	overflow	This alert indicates that a suspicious command xp_cmdshell is running on the MSSQL Server. The command when used, is highly likely to cause overflow, misused or other issues.	
MSSQL xp_reg execution	17440	medium	overflow	This alert indicates that a suspicious command xp_reg is running on the MSSQL Server. The command when used, is highly likely to cause overflow, misused or other issues.	CVE-2002-0642
MSSQL xp_sprintf execution	6	medium	overflow	This alert indicates that a suspicious command xp_sprintf is running on the MSSQL Server. The command when used, is highly likely to cause overflow, misused or other issues.	CVE-2001-0542
HTTP SQL Injection Attempt	76400	medium	sql-injection	SQL injection is a technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. It is in fact an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another.	