Securing IIS

How to implement a secure IIS web server

Allaire Security White Papers Series

(Version 1.0)

Abstract

Title	Securing IIS
Date	January 8, 2001
Product	Microsoft IIS Server
Target Audience	Web Server Administrators
Abstract	Securing a web server can be a difficult process, considering the vast number of security advisories an administrator must keep track of. This document and other lockdown documents are Allaire's efforts toward making this job a little easier.

Allaire Corporation • One Riverside Center • 275 Grove Street • Newton • MA • 02466
www.allaire.com • info@allaire.com • (617) 219-2000 •
security issues: secure@allaire.com
document feedback: lockdown@neohapsis.com

Table of Contents

Securing IIS

The intended purpose of this document is to provide a collection of the changes necessary to have a securely configured IIS server. All changes documented herein and in the Microsoft Checklist (see below) should be reviewed and evaluated for implementation on your IIS installation. Deciding to overlook suggestions may leave you with a system open to compromise. Implementing these fixes will assure that you are protected from many types of known attack.

Microsoft recommended guidelines

Microsoft regularly publishes the 'Security Checklist for IIS', which is the most thorough secure-implementation guideline available. You should use this document as a basis for a secure IIS installation. It is available from

http://www.microsoft.com/technet/security/tools.asp

At time of writing the IIS 4.0 checklist was last updated on March 15th, 2000. The IIS 5 checklist was last updated on June 29, 2000. There are a few notes about the checklists:

- Latest service pack for Windows NT 4.0 is SP6a. It is available from:

  http://www.microsoft.com/ntserver/nts/downloads/recommended/SP6/default.asp

- There are post-SP6 hotfixes already available that correct security vulnerabilities in IIS. You should periodically check for new security hotfixes and patches at:

  http://www.microsoft.com/security/bulletins/current.asp

- Virtual directory permissions for ColdFusion templates are similar to .ASP files:

  ```
  Everyone (Execute)
  Administrators (Full Control)
  System (Full Control)
  ```

- You can disable Index Server since ColdFusion comes with Verity, a replacement search/index service.

ColdFusion Installation Notes

When installing ColdFusion for use with IIS, there are a few areas you should double-check:

- You should remove the .DBM file mapping if your site does not use .DBM templates. .DBM was the old ColdFusion extension—it has been replaced with .CFM. If you do not have any .DBM files in use, you can remove the mapping by doing the following:

    - Open up the Microsoft Management Console
    - Select 'Internet Information Server'
    - Select the appropriate system
    - View the properties for the appropriate website
    - Select the 'Home Directory' tab
    - Click the 'Configuration' button under 'Application Settings'
    - Select '.dbm'
    - Click the remove button

  NOTE: while following these instructions you should also remove any other unused file mappings—in particular, examine .htr, .idc, .stm, .shtml, etc.

- Remove the 'CFExamples' and 'CFSnippets' sample DSNs. To do this:

    - Open up Control Panel
    - Select ODBC
    - Select the 'System DSN' tab
    - Select the particular DSN in question
    - Click the 'Remove' button

  NOTE: while following these instructions you should also remove any other unused DSNs—in particular, examine the 'Web SQL' and 'AdvWorks' DSNs that IIS may install by default.

- Double check the filesystem permissions on the /CFIDE/Administrator directory. Some installations give the 'Everyone' user 'Change' permission, which is incorrect. You can fix this by doing the following:

    - Navigate to the /CFIDE/Administrator directory folder
    - View the properties for the Administrator folder
    - Select the 'Security' tab
    - Click the 'Permissions' button
    - Highlight 'Everyone'
    - Change the permission to 'Read'
    - Check the 'Replace Permissions on Subdirectories' checkbox
    - Click the 'OK' button

    - When prompted, select ‘Yes’

- In production environments, you should remove the /CFDocs directory. See Allaire Security Best Practices Document 10954 at:

  http://www.allaire.com/Handlers/index.cfm?ID=10954&Method=Full

  for further details.