Global Information Assurance Certification Paper

Microsoft FrontPage 2000 Server Extension Security: An Oxymoron?

Whatever your opinion may be of FrontPage 2000 as an HTML authoring tool, among web content authors who need to get their job done quickly it is a popular tool for rapid page development. Busy system administrators who learn that they will be required to support FrontPage Server Extensions (FPSEs) often have little time to research and implement best practices for the product; sometimes, security administration is minimized to upgrading the to the latest version of the FPSEs.[1] This brief paper examines key online resources and best practices for securing FPSEs on Windows NT.

Online Resources for the Busy Administrator

For the administrator who inherits a web site that uses FPSEs, Microsoft provides several web sites with dozens of useful articles. First, security bulletins are posted on the Microsoft security site regarding vulnerabilities pertinent to Microsoft's products.[2] Second, the FrontPage section of Microsoft Developers Network offers detailed resources on the FPSE remote procedure calls (RPCs), FrontPage security, as well as UNIX and NT versions of the FPSEs available for downloading.[3] Third, a Boolean search on Microsoft TechNet for *FrontPage 2000 NEAR security* produces dozens of hits; most of these are configuration issues when using FrontPage with other products such as Site Server, Access or Windows 2000 and merit review. Three hits from the TechNet search pertain to vulnerabilities, their risks and remediation: (1) FrontPage 2000 Server Extensions remove a potential denial of service attack by deactivating a component (Dvwssr.dll) that is included with FrontPage 98 and the Windows NT 4.0 Option Pack;[4] (2) if the FrontPage author is using the Windows NT 4.0 Personal Web Server for development, a security patch is available to mitigate the risk of an attack that would violate content confidentiality;[5] and, (3) a patch is available for Office 2000 products to eliminate an ActiveX control (Ouactrl.ocx) which could be maliciously used by the operator of a remote web site to violate the integrity of a visitor's computer.[6] Since the FPSE SR1.2 was issued in August of 2000, one security bulletin has been released of a potential denial-of-service attack, exploiting vulnerability within IIS via the FPSEs; a patch is available.[7]

With any product, it is important to rely not only on the vendor but on third party sources as well, performing a cross-reference between what they and the vendor report. The choice of such third party resources is, of course, dependent on each administrator. An example of the value of such third-party resources bug reports is the case where a FrontPage Server Extension component (Shtml.exe) could be used to request a DOS device name with a .htm extension, e.g., http://www.test.com/_vti_bin/shtml.exe/prn.htm resulting in a denial of service and confidentiality breach of server path information.[8] Similarly, monitoring a service such as SANS' Global Incident Analysis Center (GIAC) detections analysis can provide useful information. For example, this past spring and early summer saw a flourish of detections around FrontPage Server Extensions, leading many administrators to examine more closely their FPSE configurations and practices.[9]

Best Practices for Administering FrontPage 2000 Server Extensions

Researching, reading and implementing information gleaned from the above online resources is but one part of administering FrontPage Server Extensions; best practices require further steps. Ideally, these steps are taken with a new web server or one that is undergoing a scheduled security audit offline. Among the essential documents to read are: (1) the FrontPage 2000 Server Extensions Resource Kit (SERK), which provides detailed information about securing them on Windows NT and UNIX;[10] (2) the Microsoft Developers Network FrontPage site provides detailed documentation about the FrontPage 2000 remote procedure calls (RPC);[11] and, (3) PriceWaterhouseCooper's FrontPage 2000 Server Extensions Security White Paper.[12] The security white paper offers a Baseline Security Configuration for both Windows NT and UNIX. Among the best practices gleaned from the white paper and SERK for Windows NT are:

1. Run only the services that are absolutely necessary;[13] if FrontPage Server Extensions' administrative and authoring capabilities are not required, do not install or uninstall FrontPage Server Extensions.

2. If the FPSEs are required, do not accept default installation options as secure enough.

3. Rename the local Administrator and Guest accounts; disable the latter.[14]

4. Set account policies to require strong passwords.[15]

5. Review and tighten directory permissions and access to the registry to harden the server.[16]

6. Grant the appropriate level of access for the FrontPage administrator:
   - this person does not need to be a member of the local Administrators group on the server;
   - create a special group to administer the web site;
   - remove from the site any groups not required for browsing, authoring or administering the site.[17]

7. Do not enable account lockout on the *IUSR_computername* account as it can lead to a denial of service attack; rather, rely on a strong password as generated for that account.[18]

8. Verify the default setting that authors cannot upload files into executable directories.[19]

9. Secure remote administration with a port other than the suggested port 8234 and require SSL for administration.[20]

10. If accessing the FPSEs through a proxy server or firewall, require SSL with Basic Authentication; if authoring behind the firewall, require NTLM authentication.[21]

11. Enable the option to "Log authoring action" and audit the _vti_log /author.log for authoring actions;[22] correlate with the web logs for suspicious activity.

12. If feasible, use the IP Address Restriction to restrict administration or authoring to a single machine or group of machines.[23]

13. Ensure that the registry key setting for ClientVerCutoff is set to the major versions number corresponding to the FPSEs on the server; administration and authoring will be permitted only with the corresponding version of FrontPage.[24]

14. Create subwebs for each area that has a web author to create content and restrict authoring access to a specific WEB*businessarea* group.[25]

15. Give careful consideration to whether or not Content Indexing is to be enabled or disabled since that content might be available inappropriately to anonymous users; it can be configured per subweb.[26]

16. Enable Version Control with the FPSEs to provide source control; monitor the FrontPage built-in reports to ensure that appropriate authors are modifying the pages. Compare the results with the author.log file.[27]

17. Ensure that the FPSE Configuration Variables are set appropriately in the Registry or, for a specific subweb, in the _vti_pvt/Service.cnf file. Setting conflicts are resolved in the order of: Subweb configuration variables have the highest priority; virtual server configuration variables have the second priority; global configuration variables have the third priority.[28] Among the forty-two configuration variables, some of the most important are mentioned above; others which need to be considered and configured for Windows NT:

Hkey_Local_Machine\SOFTWARE\Micorosoft\Shared Tools\Web server Extensions\All Ports	
AccessControl	1 (Default)
AllowExecutableScripts[29]	0 (Default)
ClientVerCutoff[30]	Vti_clientvercutoff:SX|4.0.2.0000
ListSystemsDSNs[31]	0 (Default is 1 and allows FP authors to enumerate DSNs on the server)
Logging[32]	1
NoExecutableCGIUpload[33]	1 (Default)
NoMarkScriptable[34]	1
NoSaveResultsPipeTo[35]	1 (Default)
NoSaveResultsToAbsoluteFile[36]	1 (Default)
PrivateBrowsable[37]	0 (Default)
RestrictIISUsersAndGroups[38]	1
RequireSSL	Enable only if SSL is required

RunTimeFileExtensions[39]	.htm, .html

Conclusion

It is possible to secure and administer an FPSE-enabled web; to do so, however, it requires that the administrator monitor the appropriate vendor security bulletins, third-party security sites and the FrontPage enabled web site itself. Moreover, it is critical that certain baseline configuration steps are well documented and implemented in order to ensure a web server build that can be accredited as secure for deployment in production; preferably, this is done with a new server build or with a server undergoing a regular security audit before being returned to production. The title of this paper poses a question *Microsoft FrontPage 2000 Server Extension Security: An Oxymoron?* that can be answered with a qualified 'no': a combination of reasonable research and best practices can mitigate the risks inherent with a tool like Microsoft FrontPage 2000.

---

[1] On August 15th and 29th, 2000, Microsoft released the FrontPage 2000 Server Extensions SR 1.2 for Windows and UNIX; the focus of this paper is on FrontPage 2000 Server Extensions on Windows NT. The latest versions of the FPSEs are available for download. URL: http://msdn.microsoft.com/workshop/c-frame.htm?/workshop/languages/fp/default.asp

[2] URL: http://www.microsoft.com/security. The security bulletins are issued first and are followed by an FAQ and Knowledge Base (Qxxxxxx) article. The security bulletins are available on an e-mail subscription basis, helping the administrator keep up with the latest issues.

[3] The number of hits varies as Microsoft issues patches and removes articles from their site; at the time this paper was written, ninety-four hits were returned. A close reading of all ninety-four hits reveals that the following are pertinent Microsoft's Support Knowledge Base articles for FrontPage 2000:

1. Q232645 FP2000: Configuration Settings to Assist in Securing Database Information on a Web Server
2. Q215365 Server Error: The folder "/Cgi-bin" Is Marked Executable
3. Q216705 How to Set Permissions on a FrontPage Web on IIS
4. Q216820 Check Server Extensions Grants Extra Permissions
5. Q221769 Err Msg: Server Error: FrontPage Security Violation
6. Q231856 Err Msg: PROBLEM: Your Web Is Insecure Because the Server Extensions DLLs Are Installed on a FAT Drive
7. Q237960 How to Configure FrontPage to Connect through a Raptor Firewall
8. Q260159 Errors When Viewing Permissions in FrontPage
9. Q230169 Unable to Open or Create Web Folder for Restricted FrontPage Web
10. Q272287 FPSE: UNIX-Based Fixes for Server Extensions SR 1.2
11. Q225202 Incorrect NTFS Permissions When Reducing Account to Browse (FPSE98 - Fixed with FPSE 2000)
12. Q253592 OFF2000: An Upgrade to Windows 2000 Restricts Internet Information Server (IIS) Users and Groups
13. Q240735 Resetting Multiple Virtual Server Permissions with FrontPage 2000
14. Q240736 How to Restrict Browse Access to a Folder
15. Q269835 FPSE: Windows-Based Fixes for Server Extensions SR1.2
16. Q230778 Err Msg: The Web Server Does Not Appear to Have Any Authentication Methods Enabled
17. Q207288 FP2000: How to Create a Registration Web
18. Q229286 FP2000: Cannot Connect to SQL Database on Windows NT Server Computer with IIS
19. Q265468 FP2000: Security Command Is Not Available on Tools Menu
20. Q205672 FP2000: FrontPage Does Not Accept Blank Password
21. Q197740 FP2000: What Is a Registration Web?

22. Q239833 How to Configure FrontPage Authoring with Site Server Membership
23. Q243842 FP2000: How to Create Data Access Page Linked to Access Database in FrontPage Web
24. Q219104 FP2000: Web Publishing Wizard Generates Error Publishing to Nested Sub web
25. Q216057 Unable to Open Web with Only Registered Users Have Browse Access
26. Q198118 Server Extensions Must Run in Process on IIS 4.0
27. Q236085 Server Error: Cannot Mark a Folder Executable on This Server
28. Q202323 Subwebs Created in the MMC Inherit Parent Web's Groups
29. Q238128 The Name "Groupname" is not a Valid User or Group
30. Q216150 Creating Web Causes Server Error: Administrators Is Reserved
31. Q223433 Permission Errors Occur after Upgrading to FrontPage 2000
32. Q215421 Incorrect Error Installing Server Extensions to a UNC Path
33. Q215459 Error Converting a UNC Virtual Directory to a Sub Web
34. Q238461 Err Msg: 405 Method Not Allowed
35. Q236464 HOWTO: Restrict Users and Groups in FrontPage 2000 on IIS
36. Q219650 FP2000: Lightweight Source Control Not Functioning Properly on FAT
37. Q228996 Cannot Convert Virtual Directory to Subweb Remotely
38. Q225200 FP2000: Custom Confirmation Component Displays Only Field Name If Called by Save to Database Form
39. Q265134 FP2000: FrontPage 2000 Server Extensions Service Release 1.1
40. Q230183 Posts Do Not Display If Discussion Web Uses Built-in Source Control
41. Q205245 FP2000: "Socket Code 4" Error Connecting to Server Using SSL
42. Q205254 FP2000: Web Permissions Must Be Unique to Be Modified
43. Q272542 FPSE: Cannot Open Subweb That Is Using Unique Permissions
44. Q247864 FP2000: Command-Line Arguments for Server Administrator
45. Q208637 FP2000: Registration Form Not Supported on IIS Web Server
46. Q243623 Errors Occur with Source Control Integration When Checking Out Files
47. Q264760 FP2000: Can't Save Changes After Modifying a File
48. Q230712 How to Use FrontPage Components on ASP Pages
49. Q201845 Valid Account Cannot Open Sub Web When Root Web is Restricted
50. Q264977 FP2000: You Receive an Error Message When Submitting a Form
51. Q215481 Installing FrontPage 2000 Server Extensions to Netscape UNIX Server
52. Q265207 FP2000: Users Cannot Browse a Restricted Subweb
53. Q264932 FP2000: Users Cannot Publish Changes After Installing FrontPage
54. Q265134 FP2000: FrontPage 2000 Server Extensions Service Release 1.1

[4] Q259799 FP98: FrontPage 98 Server Extensions DLL Exposes Security Vulnerability It is important for administrators to document which version of the FPSEs are running on the web servers and to follow or implement a formal change management process to upgrade them.

[5] Q217763 File Access Vulnerability in Personal Web Server and Patches for File Access Vulnerability in Personal Web Servers The articles regarding this vulnerability are a bit vague; it appears that it is the Personal Web Server 4.0 that comes with the Windows 4.0 Option Pack that is vulnerable.

[6] Q262767 OFF2000: Update Available for "Office 2000 UA Control" Vulnerability.
The first vulnerability is resolved by an upgrade to the FrontPage 2000 Server Extensions; the latter two still require separate patches which are available. URL: http://www.microsoft.com/frontpage/swupdates.htm

[7] The security bulletin for the "Malformed Web Submission" vulnerability was issued on December 22, 2000. URL: http://www.microsoft.com/technet/security/bulletin/MS00-100.asp. The FAQ is available as well. URL: http://www.microsoft.com/technet/security/bulletin/fq00-100.asp

[8] The bug was eliminated with the FPSE SR1.2 on August 15, 2000. However, according to a source at Neohapsis, this bug was reported to Microsoft on July 5, 2000. See Neohapsis comments, URL: http://archives.neohapsis.com/archives/bugtraq/2000-08/0288.html and Microsoft's reply, URL: http://archives.neohapsis.com/archives/bugtraq/2000-08/0323.html. The original vulnerability with the "Shtml.exe" was discovered by Xato Security Networks (URL:http://www.xato.net/reference/xato-082000-01.htm) SecurityPortal (URL:http://www.securityportal.com), among others offers similar bug reports.

[9] The GIAC intrusion detection analysis logs noted significant discussions around the topic:
May 16 – URL: http://www.sans.org/y2k/051600.htm;
May 28 – URL: http://www.sans.org/y2k/052800-1130.htm;
June 12 – URL: http://www.sans.org/y2k/061200.htm;
June 13 – URL: http://www.sans.org/y2k/061300.htm;
June 16 – URL: http://www.sans.org/y2k/061600.htm;
June 17 – URL: http://www.sans.org/y2k/061700.htm;
June 20 – URL: http://www.sans.org/y2k/062000.htm;
June 21 – URL: http://www.sans.org/y2k/062100.htm;
June 22 – URL: http://www.sans.org/y2k/062200.htm;
August 31 – URL: http://www.sans.org/newlook/digests/ntarchives/2.2.2

[10] FrontPage 2000 Server Extensions Resource Kit (SERK). URL:
http://officeupdate.microsoft.com/frontpage/wpp/serk/

[11] The RPC documentation is a free download in HTML format. URL:
http://msdn.microsoft.com/workshop/c-frame.htm?/workshop/languages/fp/default.asp

[12] Feinman, Todd M. and Goldman, David J. "FrontPage 2000 Server Extensions Security White Paper" PriceWaterhouseCoopers: 29 July 2000. URL:
http://msdn.microsoft.com/workshop/languages/fp/2000/FPSEsecurity.exe . This lengthy (127 pages) white paper is an indispensable read for NT and UNIX FrontPage security administrators.

[13] Ibid., 37.

[14] Ibid. 31.

[15] Ibid., 31, 44-45.

[16] Ibid., 32-35.

[17] Ibid., 16 and 18.

[18] Ibid., 21-22.

[19] Ibid., 20

[20] Ibid., 17.

[21] Ibid., 44.

[22] Ibid., 43.

[23] Ibid., 45.

[24] Ibid., 45.

[25] Ibid., 46.

[26] Ibid., 47.

[27] Ibid., 48-49.

[28] Ibid., 36. For a list of all forty-two variables, see , FrontPage 2000 Server Extensions Resource Kit. URL:http://officeupdate.microsoft.com/frontpage/wpp/serk/apndx03.htm

[29] See, FrontPage 2000 Server Extensions Resource Kit. URL: http://officeupdate.microsoft.com/frontpage/wpp/serk/apndx03.htm#AllowExecutableScripts . The default value is 0; setting it to a non-zero value will make all files executable in the directory. "If *NoExecutableCgiUpload* is set to **0** and *AllowExecutableScripts* is set to **0**, authors will be able to upload and use ASP and IDC files, but not CGI or ISAPI files." Also see, FrontPage 2000 Server Extensions Resource Kit.URL: http://officeupdate.microsoft.com/frontpage/wpp/serk/apndx03.htm#NoExecutableCgiUpload

[30] See, FrontPage 2000 Server Extensions Resource Kit. URL: http://officeupdate.microsoft.com/frontpage/wpp/serk/apndx03.htm#ClientVerCutoff Microsoft states that this variable can be enabled only on a web's _vti _pvt/Service.cnf file.

[31] The SERK states: "When FrontPage 2000 server extensions are installed on a Web server, users of the FrontPage client can list all system DSNs on the server by clicking **Web Settings** on the **Tools** menu and going to the **Database** tab. This can create a security hole, because it exposes a list of resources on your server. When *ListSystemDSNs* is set to zero, FrontPage users cannot view the list of system DSNs on the Web server. When *ListSystemDSNs* is set to a non-zero value, system DSNs are listed."
See, FrontPage 2000 Server Extensions Resource Kit. URL: http://officeupdate.microsoft.com/frontpage/wpp/serk/apndx03.htm#ListSystemDSNs

[32] FrontPage 2000 Server Extensions Resource Kit. URL: http://officeupdate.microsoft.com/frontpage/wpp/serk/apndx03.htm#Logging

[33] See endnote 24 above.

[34] The SERK states: "(IIS 4.0 or later) When *NoMarkScriptable* is set to a non-zero value, users of the FrontPage client cannot modify the scriptable bit on any folders in a web. When this value is set, an Internet service provider must manually set the scriptable bit on folders. When *NoMarkScriptable* is set to **0**, FrontPage client users can modify this bit.
Internet service providers can use this setting to selectively allow or disallow use of database features and other ASP-based pages on a per-server or per-web basis."

FrontPage 2000 Server Extensions Resource Kit. URL: http://officeupdate.microsoft.com/frontpage/wpp/serk/apndx03.htm#NoMarkScriptable

[35] This variable is to ensure that form results are not piped to an arbitrary program: "Earlier releases of FrontPage allow the default (Save Results) form handler to pipe form results to any arbitrarily chosen program. For backward compatibility, *NoSaveResultsPipeTo* disables this capability when it is set to a non-zero value. To allow piping form contents to a program, set this variable to **0**."
FrontPage 2000 Server Extensions Resource Kit. URL: http://officeupdate.microsoft.com/frontpage/wpp/serk/apndx03.htm#NoSaveResultsPipeTo

[36] "When *NoSaveResultsToAbsoluteFile* is set to **1**, the default (Save Results), Registration, and Discussion form handlers cannot write to an absolute file path even if the browsing account has the NTFS rights to write to that path: the form handlers can only write to a file within the web's content area. When *NoSaveResultsToAbsoluteFile* is set to **0**, the FrontPage default (Save Results), Registration, and Discussion form handlers will write to an absolute file path

Use *NoSaveResultsToAbsoluteFile* instead of the obsolete *NoAbsoluteFileResults*."
FrontPage 2000 Server Extensions Resource Kit. URL:

http://officeupdate.microsoft.com/frontpage/wpp/serk/apndx03.htm#NoSaveResultsToAbsoluteFile

[37] The _private/ folder can contain information that should not be browsed by the public, e.g., form results. FrontPage 2000 Server Extensions Resource Kit. URL:
http://officeupdate.microsoft.com/frontpage/wpp/serk/apndx03.htm#PrivateBrowsable

[38] This setting can restrict the FrontPage administrator's ability to view the entire domain's global groups, providing only those groups necessary for site administration. FrontPage 2000 Server Extensions Resource Kit. URL:
http://officeupdate.microsoft.com/frontpage/wpp/serk/apndx03.htm#RestrictIISUsersAndGroups

[39] This variable restricts file formats that the FPSEs can access: "When using the FrontPage Server Extensions executable Shtml.exe, versions 3.0.2.1330 or later, run-time FrontPage-based components such as the default (Save Results) form handler and the Search form will only process HTML or HTML-based files that do not contain ASP code or the SCRIPT RUNAT=server tag. This prevents exposing the contents of source code, passwords, or other private information to users.
The set of HTML or HTML-based files that can be processed by Shtml.exe is identified by file name extension: .htm, .html, .shtm, .shtml, .htx, .asp, .alx, and .asa. If the Web server's configuration file maps other filename extensions to an HTML or HTML-based file type, those files are also added to the set of files that can be processed by Shtml.exe.
... If *RunTimeFileExtensions* is not specified, Shtml.exe processes only files with .htm and .html extensions. *RunTimeFileExtensions* is ignored in versions of the FrontPage Server Extensions earlier than 3.0.2.1330."

FrontPage 2000 Server Extensions Resource Kit. URL:
http://officeupdate.microsoft.com/frontpage/wpp/serk/apndx03.htm#RunTimeFileExtensions