Microsoft IIS 0Day Vulnerability in Parsing Files (semi-colon bug)

Last Update: 25 Dec. 2009

Reason of Update: Update in version of vulnerable application

Application: Microsoft Internet Information Services - IIS (~~All versions~~ Work successfully on IIS 6 and prior versions – IIS7 has not been tested yet – does not work on IIS7.5)

Impact: Highly Critical for Web Applications

Finding Date: April 2008

Report Date: Dec. 2009

Found by: Soroush Dalili (Irsdl {4t] yahoo [d0t} com)

Website: Soroush.SecProject.com

Weblog: Soroush.SecProject.com/blog/

Thanks From: Mr. Ali Abbas Nejad, Mormoroth, Aria-Security Team, and other ethical hackers.

Vulnerability/Risk Description:

- IIS can execute any extension as an Active Server Page or any other executable extension. For instance “malicious.asp;.jpg” is executed as an ASP file on the server. Many file uploaders protect the system by checking only the last section of the filename as its extension. And by using this vulnerability, an attacker can bypass this protection and upload a dangerous executable file on the server.

Impact Description:

- Impact of this vulnerability is absolutely high as an attacker can bypass file extension protections by using a semi-colon after an executable extension such as “.asp”, “.cer”, “.asa”, and so on.
- Many web applications are vulnerable against file uploading attacks because of this weakness of IIS. In a measurement which was performed in summer 2008 on some of the famous web applications, 70 percent of the secure file uploaders were bypassed by using this vulnerability.

Method of Finding:

- Simple fuzzer by using ASP language itself.

More Details:

- In case of having the “malicious.asp;.jpg”, web applications consider it as a JPEG file and IIS consider it as an ASP file and pass it to “asp.dll”. This bug does not work with ASP.Net as the .Net technology cannot recognize “malicious.aspx;.jpg” as a .Net file and shows a “page not found” error.
- Besides using semi-colon, “:” can be used to make an empty file with any arbitrary extension. For example by uploading “test.asp:.jpg”, an empty ASP file - “test.asp” - would be created on the server on an NTFS partition. This is only because of “NTFS Alternate Data Streams” and it is completely different from the semi-colon vulnerability.

Fast Solution/Recommendation:

- **For Web Developers:**
  - Highly Recommended: Use a completely random string as a filename and set its extension by the web application itself (by using a “switch-case or select-case” for example) and never accept the user’s input as the filename.
  - Only accept alpha-numerical strings as the filename and its extension.
- **For Webmasters:**
  - Remove “execute” permission from the upload directories (folders).

Proof of Concept/Exploit:

- Many of the web applications can be exploited by using this vulnerability. We cannot announce their names before the Microsoft security patch for IIS because of security reasons.

Related Documents:

- http://www.owasp.org/index.php/Unrestricted_File_Upload
- http://www.owasp.org/index.php/File_System
- http://soroush.secproject.com/downloadable/iis-semicolon-report.pdf