

## **COT Security Alert – Microsoft IIS 0 Day Vulnerability in Parsing Files (semi-colon bug)**

---

The COT Security Administration Branch has become aware of a Microsoft IIS Zero-Day Vulnerability in Parsing Files (semi-colon bug). The risk of this vulnerability is very high as an attacker can bypass file extension protections by utilizing a semi-colon after an executable extension.

Systems Affected: Microsoft IIS 6.0 and earlier versions.

Description: A vulnerability has been discovered in Microsoft IIS which could allow an attacker to upload arbitrary files to an affected system. On web sites where file uploading is enabled, successful exploitation could enable the attacker to bypass the file type filter and result in an attacker being able to upload a malicious file onto a vulnerable system. This vulnerability is caused by the way IIS performs input validation on user-supplied filenames. Specifically, the server will allow the upload of a file with semi-colon characters after an executable extension such as ".asp".

Many web applications, particularly those which allow file uploads, only check the last portion of a filename as its extension. In an attack scenario in which the file "test.asp;.jpg" is uploaded to a web-server by an attacker, the server would accept the uploaded file as a harmless image. However, once the file is on the system, the server will render the file as an ASP page. If "Execute Scripts and Executables" permission is enabled for the site and depending on the privileges associated with the service, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

### Suggestions 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. Always validate and sanitize input.

Only accept alpha numerical strings as the filename and its extension.

### Suggestions For Webmasters:

Remove "execute" permission from the IIS web directories where file upload is enabled.

Restrict file uploads to trusted users only.

Other Recommendations:

**There is currently no patch available for this exploit.** Please ensure all servers remain current with the latest patches and updates to ensure that the patch is installed as soon as one is available.

References:

Secunia: <http://secunia.com/advisories/37831/>

Security Focus: <http://www.securityfocus.com/bid/37460>

Vupen: <http://www.vupen.com/english/advisories/2009/3634>

Microsoft: <http://blogs.technet.com/msrc/archive/2009/12/27/new-reports-of-a-vulnerability-in-iis.aspx>

If you suspect a compromise of your systems please contact:

[\*\*COTSecurityServicesISS@ky.gov\*\*](mailto:COTSecurityServicesISS@ky.gov)

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Security Administration Branch  
Commonwealth Office of Technology  
120 Glenn's Creek Road, Jones Building  
Frankfort, KY 40601

[\*\*COTSecurityServicesISS@ky.gov\*\*](mailto:COTSecurityServicesISS@ky.gov)

[\*\*http://technology.ky.gov/security/\*\*](http://technology.ky.gov/security/)

