**Security Misconfiguration**

**SEVERITY:** **MODERATE HIGH**

**VULN. CODE:** SEC-MISC

**AUTH. REQUIRED:**

**VULNERBAILITY DESCRIPTION**

Following the analysis activity, a misconfiguration emerged concerning the system that hosts the application software in operation. The misconfiguration detected is related to the following issues:

* file names supported by the HTTP service and accepted by the system: the presence of the 8dot3 option in the creation of files on the NTFS filesystem has been detected;
* methods supported by the HTTP service and accepted by the system: the presence of the OPTIONS method has been identified.

**8dot3 ENUMERATION**

During the analysis it was found that the NTFS file system in use on the operating system that hosts the web server has the function 8dot3NameCreation enabled. This function creates a short filename in the 8.3 convention (8 characters’ name. 3 characters’ extension), i.e. the files in the file system are accessible both by their full name and by the short name. This vulnerability allows an external threat agent to enumerate the files present on the file system and accessible via the web server, as shown in **Box 1**.

|  |
| --- |
| $ java -jar iis\_shortname\_scanner.jar 10.10.10.191 |

**Box 1 – 8.3 enumeration result**

**INSECURE HTTP VERBS**

HTTP methods considered insecure or unnecessary that have not been disabled have been recognized via the OPTIONS method, which can be executed by any unauthenticated user, and are listed, as follows, in the "Allow" response field:

|  |
| --- |
| Allow: GET, POST, OPTIONS, HEAD, MKCOL, PUT, PROPFIND, PROPPATCH, DELETE, MOVE, COPY, GETLIB, LOCK, UNLOCK |

**Box 2 - List of used and recognized methods**

**SUGGESTED SOLUTIONS**

It is recommended to disable the creation of short names in the 8.3 convention on the NTFS filesystem.

This option can be set by changing the value of the registry key

HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\ NtfsDisable8dot3NameCreation

Please note that this option does not change the files, but changes the way the NTFS file system handles and displays the files.

It is also recommended to disable the HTTP OPTIONS/PUT/DELETE/TRACE methods if not used and necessary on the web server.

**REFERENCES**

More information regarding the vulnerability and its possible solutions can be found on the following addresses:

**REF 1 – technet.microsoft.com/en-us/library/cc959352.aspx  
REF 2 – projects.webappsec.org/Server-Misconfiguration  
REF 3 – msdn.microsoft.com/en-us/library/ff648653.aspx   
REF 4 –** [**www.owasp.org/index.php/Testing\_for\_HTTP\_Methods\_and\_XST\_(OWASP-CM-008)**](https://www.owasp.org/index.php/Testing_for_HTTP_Methods_and_XST_(OWASP-CM-008))