${FINDING\_NAME}  
**Dread Score Summary                                                         STATUS:** CONFIRMED

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | **Risk Rating** | | | | MODERATE | | | | | Damage Potential | Reproducibility | Exploitability | Affected Users | | Discoverability | Total | Remediation Effort | | 5 | 3 | 3 | ${CRI\_AFEC} | | 6 | ${CRI\_TTL} | LOW | |

**Summary of Finding**  
${CRITICAL\_SUMMARY}  
**Proof of Concept**  
${CRITICAL\_PROOF}  
**Recommendations**  
The following recommendations help ensure that unintentionally access to sensitive information or propriety data stored in publicly accessible directories is prevented.
? Turn off the Automatic Directory Listing feature in whatever application server package that you utilize.
? Restrict access to important files or directories only to those who actually need it.
? Ensure that files containing sensitive information are not left publicly accessible.
? Don't follow standard naming procedures for hidden directories. For example, don't create a hidden directory called "cgi" that contains cgi scripts. Obvious directory names are just that...readily guessed by an attacker.
Recommendations include restricting access to important directories or files by adopting a "need to know" requirement for both the document and server root, and turning off features such as Automatic Directory Listings that provide information that could be utilized by an attacker when formulating or conducting an attack.
Apache
Disable web directory browsing for all directories and subdirectories
In your httpd.conf file, disable the "Indexes" option for the appropriate Directory tag by removing it from the Options line.
In addition, you should always make sure that proper permissions are set on all files and directories within the web root (including CGI scripts and backup files). Do not copy files in the web root unless you want these files to be available over the web. Periodically go through your web directories and clean out any unused, obsolete, or unknown files and directories.
IIS, PWS, Microsoft-IIS, Internet Information Server, Internet Information Services, Microsoft-PWS
Disable web directory browsing for all directories and subdirectories
In the Internet Information Services control panel or MMC, choose the appropriate virtual directory entry and select Properties. Uncheck the 'Allow Directory Browsing' option.
In addition, you should always make sure that proper permissions are set on all files and directories within the web root (including CGI scripts and backup files). Do not copy files in the web root unless you want these files to be available over the web. Periodically go through your web directories and clean out any unused, obsolete, or unknown files and directories.
Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote
Disable web directory browsing for all directories and subdirectories
Edit Tomcat's web.xml file. In the "default" servlet, change the "listings" parameter from "true" to "false". Restart the server.
In addition, you should always make sure that proper permissions are set on all files and directories within the web root (including CGI scripts and backup files). Do not copy files in the web root unless you want these files to be available over the web. Periodically go through your web directories and clean out any unused, obsolete, or unknown files and directories.