



Cryptography_PoorEntropy_Finding - Findings Report

Oct 26, 2007 7:07:24 PM

Classification	Type	Severity	File	Line	CWE ID	SmartTrace
Vulnerability	Cryptography.PoorEntropy		Z:\jspwiki\JSPWiki_2_4_104\JSPWiki-src\src\com\ecyrd\jspwiki\filters\SpamFilter.java	262	330	
<div> <div>Description:</div> <div>The UniqueID generation for the spam filter is not truly random.</div> <div>Recommendation:</div> <div>Instead use java.security.SecureRandom().</div> </div> <div> <pre> StringBuffer sb = new StringBuffer(); Random rand = new Random(); for(int i = 0; i < 6; i++) { char x = (char)('A'+rand.nextInt(26)); sb.append(x); } return sb.toString(); </pre> </div>						
Vulnerability	Cryptography.PoorEntropy		Z:\jspwiki\JSPWiki_2_4_104\JSPWiki-src\src\com\ecyrd\jspwiki\TextUtil.java	773	330	
<div> <div>Description:</div> <div>Generation of random passwords, on password changes and administrator initial password uses an insecure source of randomness.</div> <div>Recommendation:</div> <div>Instead use java.security.SecureRandom().</div> </div> <div> <pre> // other. So, for example, omit o O and 0, 1 l and L. String letters = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ23456789+@"; String pw = ""; for (int i=0; i<PASSWORD_LENGTH; i++) { int index = (int)(RANDOM.nextDouble()*letters.length()); pw += letters.substring(index, index+1); } return pw; } </pre> </div>						