

[VulnWatch] PasswordSafe 3.0 weak random number generator allows key recovery attack

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2006-03/msg00012.html>

- *From:* vkatalov@xxxxxxxxxxxxxx
 - *Date:* Thu, 23 Mar 2006 17:14:54 +0300
-

Title : PasswordSafe 3.0 weak random number generator allows key recovery attack
Date : March 23, 2006
Product : PasswordSafe 3.0
Discovered by : ElcomSoft Co.Ltd.

Overview

=====

PasswordSafe is a program originally written by security expert Bruce Schneier (<http://www.schneier.com>) that allows one to store users' passwords in single file (called "safe") which is encrypted and protected by user's master password (called "Safe Combination") with the Blowfish encryption algorithm. As noted on PasswordSafe web page, "the program's security has been thoroughly verified by Counterpane Labs under the supervision of Bruce Schneier, author of Applied Cryptography and creator of the Blowfish algorithm."

As noted in "Password Safe FAQ", "there is no back door in PasswordSafe to recover your Safe Combination, but there is a password-guessing program that some people have used successfully. The program works by going through a list of possible passwords and checking each one".

Version 3.0 introduces new password database format which (theoretically) eliminates security flaw found by ElcomSoft Co. Ltd. in November 2005, and does not allow an attacker to bypass key stretching algorithm any more.

However, there is even more serious security flaw in version 3.0, which allows to recover 256-bit database encryption key in a reasonable time (under certain conditions). And with the recovered encryption key, it is to decrypt all database records (logins, passwords, etc) without the master password (so-called "Safe Combination").

Details

PasswordSafe 3.0 utilizes two different random number generator (RNG) functions: Win32 API RtlGenRandom() and standart Visual C++ rand(). RtlGenRandom() is not available on Windows prior to Windows XP (i.e. Windows 2000, Windows NT, Windows Me) so rand() is used instead. Specifically, rand() is used to generate 256-bit database encryption key. It is widely known that using rand() in cryptographic applications is not secure due to its predictbility and small internal state.

It is possible to mount guaranteed decryption attack on PasswordSafe 3.0 databases created under OS prior to Windows XP. The attack is very simple:

1. Generate 256-bit key for every possible seed value
2. Decrypt first database record (the structure is documented, so we have known plaintext attack)
- 3) Check decrypted value against the known plaintext

The total number of all possible seed values is limited by 2^{32} , so it is quite feasible. Our experiments show that the key can be recovered in less than 6 hours on the single PC (Pentium 4).

Impact

PasswordSafe is used to store sensitive data, and so the presence of such flaws may help attacker to disclose user's logins, passwords and PINs by implementing efficient key recovery attacks.

Solution/workaround

PasswordSafe should not use rand() function; cryptographic RNG should be used instead.

References

Bruce Schneier – Password Safe
<http://www.schneier.com/passsafe.html>

Password Safe – Project Info
<http://passwordsafe.sourceforge.net/>

Password Safe FAQ

[VulnWatch] PasswordSafe 3.0 weak random number generator allows key recovery attack

<http://www.schneier.com/passsafe-faq.html>

BugTraq: Schneier's PasswordSafe password validation flaw
<http://www.securityfocus.com/archive/1/416873/30/0/threaded>

About ElcomSoft Co.Ltd.

=====

Since 1990, ElcomSoft Co.Ltd. (<http://www.elcomsoft.com>) has been developing and marketing password recovery, forensics, and security software for Windows. The company offers a comprehensive line of password recovery software for more than 80 popular file and document types, email clients, compression programs, instant messengers, and other applications. ElcomSoft tools are used by most of the Fortune 500 corporations, many branches of the military all over the world, foreign governments, and all major accounting companies.