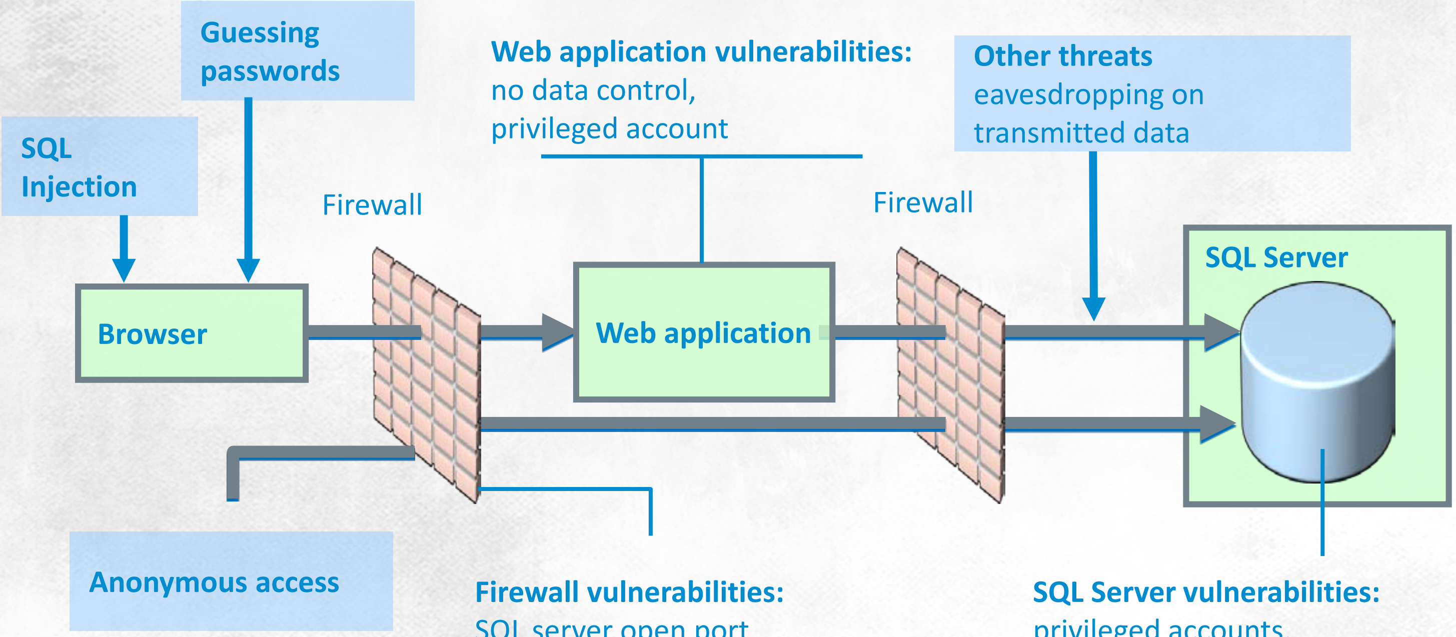
Program security assessment

Unsafe programs

By and large, administrators cannot fix insecure programs that run in their networks: all they can do is report the problem to software vendors and hope they will respond with a security patch



SQL Server vulnerabilities:
privileged accounts,
weak passwords, no auditing

Unsafe Programs

Embedding passwords in code

Fundamental errors of this type are still a reality even in newly released software

If a password is permanently stored inside an application code, it is extremely hard to change and quite easy to intercept

Even if a program uses this embedded info internally, there are widely available tools that can make it easy for an attacker obtain these passwords

```
int VerifyAdmin(char *password) {
if (strcmp(password, "TR45jhNM<1s!")) {
printf("Incorrect Password!\n");
return(0)
}
printf("Entering Diagnostic Mode...\n");
return(1);
}
```

Unsafe programs

Generic, default or blank passwords

If your manual reads: "After installation, your administrator password is QWECD$%#" or "Please submit sa as username and KJH*(&tf as password and click OK", or if you call a software support centre and are told the default admin password is JKLHUIY4, you should change all the passwords this program uses right away

CIRT.net suspic

Home

Default Passwords

461 vendors, 1895 passwor

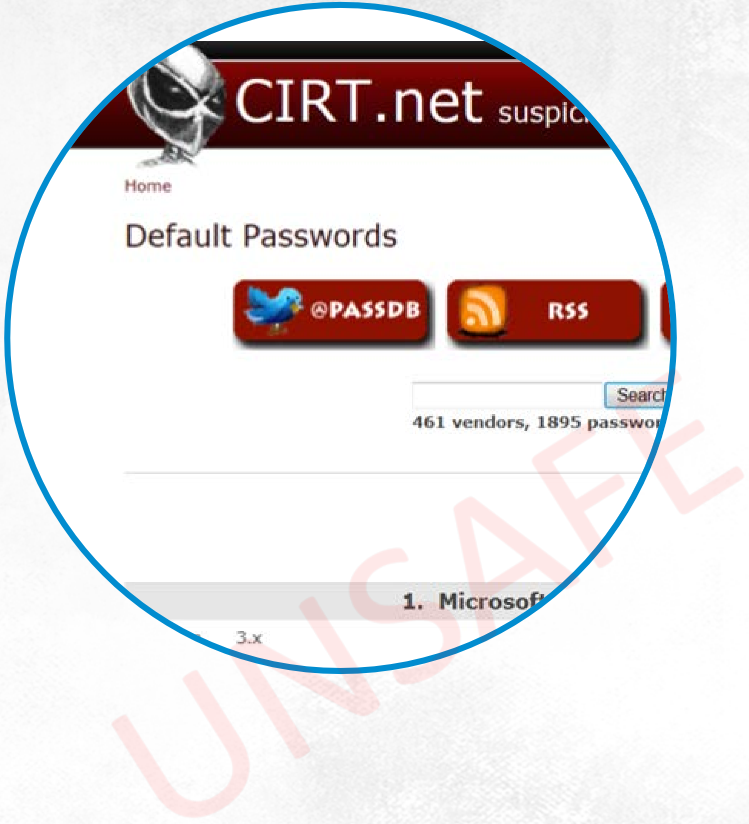
1. Microsof

3.x

Unsafe programs

Generic, default or blank passwords

Until you make sure to do this, what you have on your hands is a program that may be handling and processing confidential, critical data that everyone who's bought the same application knows the password to



CIRT.net suspic

Home

Default Passwords

461 vendors, 1895 passwor

1. Microsof

3.x

Unsafe programs

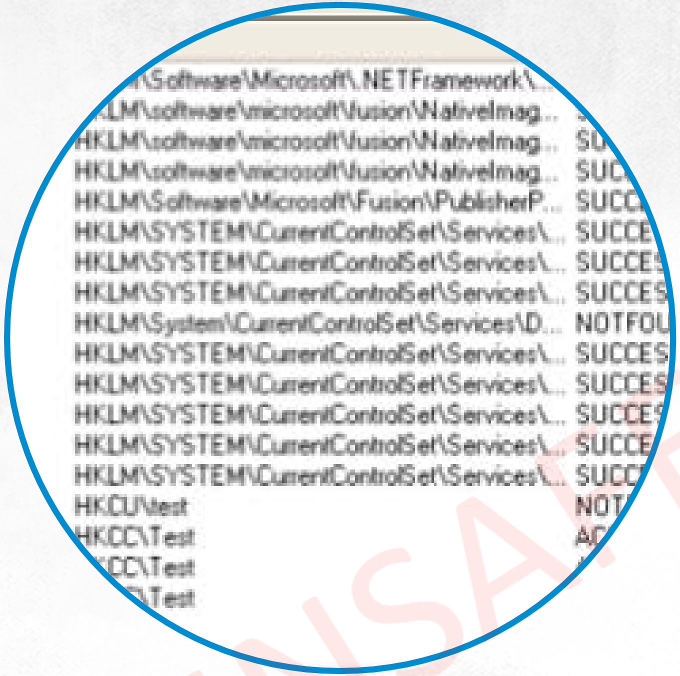
Requiring admin privileges

Some applications may not run, or at least may not run correctly, when launched by standard users

Most of these problems occur as a consequence of failed attempts to load a file, folder or system registry

If the vendor doesn't plan to release a fix, you can modify the rights to the objects the program uses by yourself:

- Launch a registry monitoring program (RegMon), a process monitor (FileMon) and the faulty application
- Capture a failed access attempt the application makes
- Grant standard users privileges to the objects used by the application

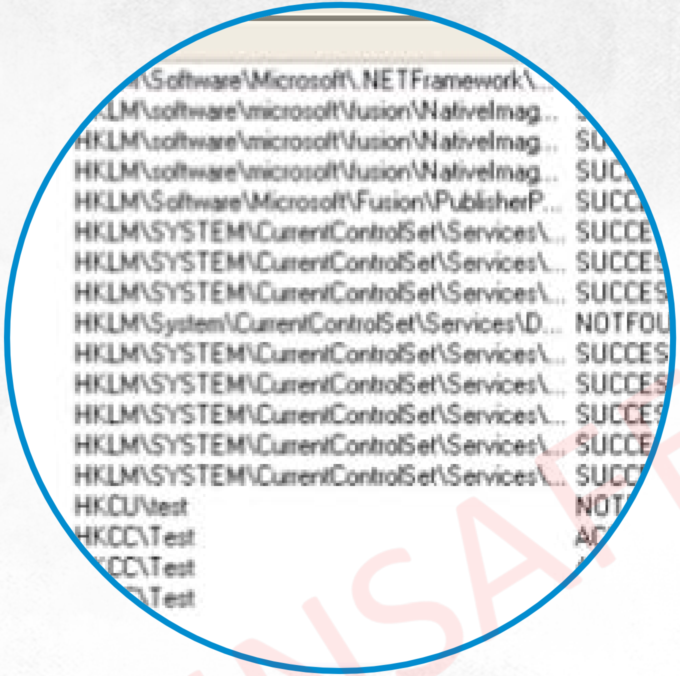


```
\Software\Microsoft\.NETFramework\...
LM\software\microsoft\fusion\NativeImag...
HKLM\software\microsoft\fusion\NativeImag...   SU
HKLM\software\microsoft\fusion\NativeImag...   SUC
HKLM\Software\Microsoft\Fusion\PublisherP...   SUCC
HKLM\SYSTEM\CurrentControlSet\Services\...     SUCCE
HKLM\SYSTEM\CurrentControlSet\Services\...     SUCCES
HKLM\SYSTEM\CurrentControlSet\Services\...     SUCCES
HKLM\System\CurrentControlSet\Services\D...    NOTFOU
HKLM\SYSTEM\CurrentControlSet\Services\...     SUCCES
HKLM\SYSTEM\CurrentControlSet\Services\...     SUCCES
HKLM\SYSTEM\CurrentControlSet\Services\...     SUCCES
HKLM\SYSTEM\CurrentControlSet\Services\...     SUCCE
HKLM\SYSTEM\CurrentControlSet\Services\...     SUCC
HKCU\test                                      NOT
HKCC\Test                                      AC
KCC\Test
\Test
```

Unsafe programs

Requiring admin privileges

```
HANDLE hFile;
hFile = CreateFile("MYFILE.TXT",           // open MYFILE.TXT
          FILE_ALL_ACCESS,        // Full control
          FILE_SHARE_READ,        // share for reading
          NULL,                   // no inheritance
          OPEN_EXISTING,          // existing file
          FILE_ATTRIBUTE_NORMAL,  // normal file
          NULL);                  // no attr. template
```



```
\Software\Microsoft\.NETFramework\...
KLM\software\microsoft\fusion\NativeImag...
HKLM\software\microsoft\fusion\NativeImag...  SU
HKLM\software\microsoft\fusion\NativeImag...  SUC
HKLM\Software\Microsoft\Fusion\PublisherP...  SUCC
HKLM\SYSTEM\CurrentControlSet\Services\...   SUCCE
HKLM\SYSTEM\CurrentControlSet\Services\...   SUCCES
HKLM\SYSTEM\CurrentControlSet\Services\...   SUCCES
HKLM\System\CurrentControlSet\Services\D...  NOTFOU
HKLM\SYSTEM\CurrentControlSet\Services\...   SUCCES
HKLM\SYSTEM\CurrentControlSet\Services\...   SUCCES
HKLM\SYSTEM\CurrentControlSet\Services\...   SUCCES
HKLM\SYSTEM\CurrentControlSet\Services\...   SUCCE
HKLM\SYSTEM\CurrentControlSet\Services\...   SUCC
HKCU\test                                     NOT
HKCC\Test                                     AC
KCC\Test
\Test
```

UNSAFE

Unsafe programs

OS update incompatibility

If you find the following info in an application’s documentation, this program is absolutely a big threat to the security of the entire system:

- Our engineering has not got chance to test these updates so they are not supported. If the customer is in urgent need to install these updates, I suggest you to set up a test system and try it.
- There are known problems with the program after you install the security update outlined in KB XYZ
- You can no longer use feature X after installing Service Pack 3

Unsafe programs

OS update incompatibility

The best solution here is to stop using these programs, at least until the vendors realise that exposing clients to danger is a financially risky practice

Windows XP SP3 and Office 2003
Support Ends April 8, 2014

THANKS