C static code analysis: Changing directories improperly when using "chroot" is security-sensitive

2-3 minutes

The purpose of creating a jail, the "virtual root directory" created with chroot-type functions, is to limit access to the file system by isolating the process inside this jail. However, many chroot function implementations don’t modify the current working directory, thus the process has still access to unauthorized resources outside of the "jail".

Ask Yourself Whether

- The application changes the working directory before or after running chroot.
- The application uses a path inside the jail directory as working directory.

There is a risk if you answered no to any of those questions.

Recommended Secure Coding Practices

Change the current working directory to the root directory after switching to a jail directory.

Sensitive Code Example

The current directory is not changed with the `chdir` function before or after the creation of a jail with the `chroot` function:

```
const char* root_dir = "/jail/";
chroot(root_dir); // Sensitive: no chdir before or after chroot, and missing check of return value
```

The `chroot` or `chdir` operations could fail and the process still have access to unauthorized resources. The return code should be checked:

```
const char* root_dir = "/jail/";
chroot(root_dir); // Sensitive: missing check of the return value
const char* any_dir = "/any/";
chdir(any_dir); // Sensitive: missing check of the return value
```

Compliant Solution

To correctly isolate the application into a jail, change the current directory with `chdir` before the `chroot` and check the return code

of both functions:

```
const char* root_dir = "/jail/";

if (chdir(root_dir) == -1) {
  exit(-1);
}

if (chroot(root_dir) == -1) {  // compliant: the current dir is changed to the jail and the results of both functions are checked
  exit(-1);
}
```

See

- OWASP Top 10 2021 Category A5 - Security Misconfiguration
- OWASP Top 10 2017 Category A5 - Broken Access Control
- MITRE, CWE-243 - Creation of chroot Jail Without Changing Working Directory
- man7.org - chdir
- man7.org - chroot

Available In: