The World of Security Misconfiguration

This article will discuss Security Misconfiguration: what it is, how it happens, and why it's dangerous.

What Is Security Misconfiguration?

Modern software is incredibly configurable, beyond what might be obvious from a look at the settings menu. The Firefox browser, for example, has over 4700 separate parameters which can be configured to control how the browser behaves. This reconfigurability lets us do more with fewer pieces of software. Rather than having to modify the code of a program whenever we want it to do something slightly different, we can just change its configuration. However, this reconfigurability also comes with some drawbacks. It can be harder to configure the software to be as secure as possible - and easier to accidentally make changes that hamper security. Such drawbacks create Security Misconfiguration, and improper software configuration reduces overall security.

Security Misconfiguration can take on many different forms, and usually (but not always), it's not as simple as setting `secure=false` in a configuration file somewhere. Security Misconfiguration also includes things like:

- **Disabled security features**: These features are the most straightforward example of where a security feature is turned off. Maybe there's a good reason, maybe there isn't, but it still degrades security.
- **Unnecessary software or features**: Whether an entire program on a web server or an optional addon that exists but is not used, unnecessary features just add more things that can go wrong.
- **Use of default credentials**: Despite being a known issue for decades, using default credentials continues to be an issue. Some software still has default admin accounts with `admin/admin` as the username and password, which is one of the first credentials an attacker will try.
- **Exposing too much information with error messages**: The issue here is less noticeable than in the other examples to show how misconfiguration can be subtle. Error messages can contain helpful information for attackers. It's usually possible to limit what information is displayed using software configuration.

Why Does Security Misconfiguration Happen?

There are two basic ways that Security Misconfiguration happens. The first and more apparent is when someone changes software configuration that harms security, such as turning off an important security feature. While this might sound far-fetched, it's more common than you think. Firstly, modern software tends to have a lot of configurable options, and it's easy to make a change without fully understanding the security implications of that change. Also, there's usually a balance that must be struck between security and usability, and it's easy to get that balance wrong when configuring software.

The second way Security Misconfiguration happens is an issue that's persisted since the early days of computer security; insecure default configurations. As before, a balance must be struck between security and usability when configuring software. Such balance is something that needs to be taken into account when deciding on default software configurations too. It would be nice if all software came configured correctly out of the box, but that's just not how things work, and it can be dangerous to assume that a piece of software's default configuration is secure.

Why Is Security Misconfiguration Dangerous?

As with many types of vulnerability, Security Misconfiguration can have many consequences. The consequences can be critical in a worst-case scenario like an unsecured admin account. In other cases, such as exposing too much information through error messages, the results are less severe but still exist. Moreover, these small misconfigurations can combine multiplicatively, reducing overall security by more than the sum of their severity.

Whether big or small, Security Misconfiguration makes attackers' lives easier, which is something we want to avoid.

Conclusion

Security Misconfiguration is a vulnerability where improper software configuration leads to degraded security. Its prevalence is partly caused by modern software's configurable features, making it more difficult to configure for security properly. It can be caused by insecure default configurations or by changing configurations to make software less secure. As a result, this makes Security Misconfiguration dangerous because, even if an individual instance of misconfiguration isn't severe on its own, they can work together to weaken overall security greatly.