Abstract

Stack overflow is one of the most common security vulnerabilities in software systems. It occurs when a program tries to load more data in a buffer than its allocated limit. It may result in serious security issue when a program having the vulnerability is run with administrator privileges. Attackers can inject malicious code into the running program through overflowing its stack. When the malicious code is executed, it allows the attackers to take control of the program. So, this security vulnerability is considered as one of the easiest and reliable techniques to gain unauthorized access to a computer system. In this article, it has been shown that how stack overflow occurs in a software system. Besides, a survey has been conducted on three popular open source projects - Linux, Git and PHP. The survey results show that the projects contain such code portions in which it is possible to overflow the stacks and inject malicious script to harm the normal execution of processes. In addition, this article raises a concern to avoid writing such codes which are potentially sources for the security attack.
References

20. Pincus, Jonathan, and Brandon Baker. "Beyond stack smashing: Recent advances in

Index Terms

Computer Science
Security

Keywords