Cybersecurity Information Technology
Kennedy Space Center

Student Name: Sairy Cohen

Academic Level: Undergraduate Junior

Academic Major: B.S. Computer Science, Mathematics minor
Academic Institution: University of Texas at El Paso

Mentor Name: Robert G. Van Arsdalen

Title: NE Information System Security Officer Org

Code/Branch: (NE-XC) Computer Systems Division: Computer Systems

Directorate: Engineering and Technology

COTS = Commercial Off The Shelf
CVE = Common Vulnerabilities and Exposures
KSC = Kennedy Space Center
NASA = National Aeronautics and Space Administration
SCCS = Spaceport Command and Control System
SIEM = Security Information and Event Management

Abstract

As technology and security measures improve, hackers keep looking for new techniques and vulnerabilities that allow them to gain access to sensitive data. This includes but is not limited to: user accounts, personal information, databases, operating systems, developmental and testing systems, and operational systems. A hacker is an individual that uses technology such as computers, tablets, and phones for unauthorized access to data. As technology becomes more robust at preventing known attacks, new vulnerabilities always exists. These vulnerabilities usually go unnoticed by developers and could potentially be exploited by an attacker. To prevent hackers from stealing sensitive and potentially harmful information, we must protect our systems and data against these criminals by developing new methods to mitigate the damage caused by these vulnerabilities and prevent them from occurring in the first place. An excellent way to discover how hackers compromise systems is by identifying and analyzing existing vulnerabilities and patching them.

The National Aeronautics and Space Administration (NASA) is one of the many federal agencies that operates under a constant threat by hackers. NASA puts a tremendous amount of effort to maintain and improve their security measures, protect critical systems, and secure sensitive information from attackers who would attempt to use it against our nation's interests.

Objectives

The NASA Engineering Information Technology (IT) Security branch at KSC serves to provide information technology security to the Engineering Directorate. Securing the systems is done by scanning their networks, patching the systems, creating vulnerability reports, and monitoring their network, vulnerabilities, firewalls, malicious code and security protocols at all times. This helps unauthorized individuals who could be considered insiders or outsiders to gain access to sensitive or confidential information.

Cyber security tools are essential for protecting information and play a highly important role defending against compromise. Within the SCCS operational and development environments,

computers are protected by COTS applications used to prevent malicious code attacks and prevent vulnerabilities from being exploited. The COTS applications generate reports which are analyzed by System Security Engineers as part of a continuous monitoring process. The COTS reports are used to inform a security team of the types of vulnerabilities that an attacker is attempting to exploit to compromise systems. This information will later be used to mitigate these vulnerabilities and determine if there are exploits or other information that may be useful to hackers. With this information, we can continue installing and patching necessary software to protect the system.

Patching takes place when the system needs to install available updates. In some cases, this may occur when the engineers maintaining the software find and fixed a "bug" in the code that can be utilized by a hacker to exploit systems. In other cases, the engineers have made updates improving the usability or performance.

Cyber Security Internship – Cyber Security Analyst

Spectre and Meltdown vulnerabilities were discovered this January, affecting every computer chip created in the last 20 years.

A. What is a vulnerability?

A vulnerability is normally a flaw in a system where hackers – unauthorized users - use to access, compromise, or steal data. It is important to understand the vulnerabilities that a computer may have in order to fix them and update and protect any sensitive information that may exist. NASA maintains a COTS application that allows System Security Engineers to learn more about the vulnerabilities a system may contain. By creating vulnerability reports, the reports provide data on the system machines to determine the vulnerability, a recommended solution, and the date when the vulnerability was published. These vulnerabilities are categorized in a level range of “Info”, “Low”, “Medium”, “High”, and “Critical”. The computers are then patched and the system continues monitoring and detecting any vulnerabilities.

B. Spectre

Spectre is a cache-based vulnerability that is used to access user’s encrypted information, such as passwords, credit card numbers, and other sensitive information. Spectre allows malicious programs to steal data while it is waiting to be processed by the computer. Spectre breaks the isolation between different applications. It allows an attacker to trick error-free programs, into leaking their secrets. Most browsers can be vulnerable and a website can read and stored that information in your browser and provide that information to another website, because JavaScript embedded in websites can be exploited via timing attacks.

One such advancement is speculative execution, which is widely used to increase performance and involves having the CPU guess likely future execution directions and prematurely execute instructions on these paths.

Imagine the following scenario:

```
void funA( int a){
        if (a == 0)
          return funX();
        else
          return funY();
    }
```

We know that one must be true; the CPU will compute both of the functions simultaneously, saving time in the process. The computer will need to prove that you are the user by asking to provide a username and password to access your information, and to confirm that you are the correct "user" but since these two functions are going at the same time the information will go to the cache memory where approval is not needed, and the data is accessible and compromised.

Project

I've been using the RedHat Linux from terminal command shell to find different ways to exploit the system and try to find sensitive information. By breaking the isolation between different applications will allow me to access unauthorized information. I analyzed the logs, conducted scanning, researched CVE, and ran reports to understand what the vulnerabilities are, and how to patch them.

Conclusion

My project consisted of collecting data and events to understand how the spectre exploit works. I'll keep working with a Linux system that will collect logs, which will be forwarded to the server for continued collection. The SIEM will then take this data and display it in dashboards. My goal is to exploit the Linux device with several commands via spectre. I will watch if NASA's security software provide alerts or discovers the intruder.

Acknowledgements

I would like to start by thanking Aqil Assalil, who played a very important role in this internship. He provided his time to teach me a lot of material and provided support and guidance. He not only played a professional role but also provided life suggestions, tips, advice, and guidance. Thank you to Aqil, for teaching me more and more every day and for taking time off you his

busy schedule to make time for me to learn new stuff. I would also like to thank my mentors Rob Van Arsdalen and Jerrace Mack for believing in me and allowing me to be part of this internship at the Kennedy Space Center.

Credits

Cohen, Sairy. "Cyber Security Information Technology Support Spaceport Command & Control System Kennedy Space Center" August 2017.