IE2012-Systems and Network Programming

Registration number	Student name
IT22899606	Anugi Ihansa Arrawwala

submission date
: 06/11/2023

CONTENT

Acknowledgment

I would like to express my special thanks to our mentor Mr.Lakmal sir, Mr. Tharaniyawarma sir & Mr, Kohilan sir for their time and efforts they provided throughout the year. Your useful advice and suggestions were really helpful to me during the project's completion. In this aspect, I am eternally grateful to you.

I would like to acknowledge that this project was completed entirely by me and not by someone else.

Vulnerability

A flaw or weakness in a system's management, design, or implementation that could be exploited to circumvent the system's security policy is called a vulnerability. Cybercriminals use a number of techniques to locate and take advantage of these vulnerabilities. Different kinds of malicious software target weaker systems with the intention of compromising them and making them act strangely. Once a vulnerability is exploited, a cyberattacker can install malware, run malicious code, and even extract sensitive data. Updates and patches from the developer, however, can address these issues.

Exploit

A program, piece of code, set of instructions, or collection of data that is created with the intention of compromising a system or exploiting a vulnerability to force it to do an action against its intended purpose is called an exploit. It takes use of a flaw or security breach in a software or computer system, usually with malicious intent, such as installing malware. An exploit is a method that cybercriminals use to distribute malware; it is not malware per se. A lot of vulnerabilities require an attacker to initiate a series of dubious actions in order to prepare an exploit for deployment. Software or system design flaws are usually the root cause of most vulnerabilities. Attackers write their malware with the express purpose.

1.CVE-2017-0144 (Eternal Blue)

1.1 Introduction

The U.S. National Security Agency (NSA) created MS17–010, also referred to as the "Eternal Blue vulnerability," which was made public on April 14, 2017, by the hacker collective known as The Shadow Brokers. When the Shadow Brokers gained access to an NSA collection of cyberweapons, they disclosed information that included Eternal Blue. The NSA faced difficulties and humiliation as a result of Shadow Brokers' online release of Eternal Blue. After being alerted, Microsoft quickly released a security update for Windows system administrators. People using outdated Windows versions or unpatched PCs were left open to assault.

Although Windows 7 and 10 were the most popular versions at the time, Windows XP was still in use by a number of sizable enterprises. Just a few weeks after details of the NSA vulnerability came to light, Microsoft responded to an alert from the agency by patching Windows 7 and 10 during the WannaCry attack. After that, Microsoft released a patch for Windows XP, which was not supported at the time [1].

A flaw that has persisted over the previous four years. The WannaCry ransomware attack, which was later used to exploit the Eternal Blue vulnerability, severely damaged the computer systems of all UK hospitals and quickly spread to the rest of the world, infecting millions of computers in a matter of days.

1.2 Methodology

Blue Kill is a tutorial that uses the Metasploit framework to exploit the Eternal Blue Vulnerability on a Windows server platform through the use of a Kali virtual machine. It is an offensive strategy since a penetration tester like Kali uses a flaw in early versions of Windows called MS17010 to get remote access to the target system. This tutorial shows the user how to use Kali's pre-installed Metasploit framework to successfully breach a Windows server that is susceptible to attack. In order to make the flags accessible to individuals who successfully demonstrate how to infiltrate the vulnerable Windows server using the Kali virtual machine, two CTFs are concealed inside the system. The primary audience for this tour is lovers of cyber security, pentesters, and newcomers to the field of cybercrime.

A flaw in Microsoft's implementation of the Server Message Block (SMB) Protocol is exploited by Eternal Blue. This approach can be used to deceive a Windows PC that has not been patched against the vulnerability into opening the door for unauthorized data packets to access the legitimate network. These data packets could include malware, such as a trojan horse, ransomware, or another potentially dangerous program.The Server Message Block version 1 (SMBv1) flaws that are present in earlier iterations of Microsoft's operating systems, including as Windows 95, Windows 98, Windows Me, Windows NT, Windows 2000, and Windows XP, are the source of the Eternal Blue attack.

2.CVE-2023-3881

2.1 Introduction

A major vulnerability was discovered in the Campcodes Beauty Salon Management System 1.0. This vulnerability affects an unidentified feature of the /admin/forgot-password.php file. SQL injection results from altering the contactno parameter. Launching the attack remotely is possible. The public has been made aware of the exploit, which is usable. This vulnerability's related identifier is VDB-235243.

2.2 Methodology

Given the extensive usage of WinRAR, the vulnerability CVE-2023-38831 presents a serious risk. This vulnerability can be used maliciously by adversaries, which makes early identification even more important. Potential damage can be reduced by identifying and countering these strikes early on. Early detection and mitigation capabilities are provided by Logpoint Converged SIEM, which provides a solution. Our platform combines native endpoint agent (AgentX), UEBA, SOAR, and SIEM for quick Threat Detection, Investigation, and Response (TDIR).

An effective tool that helps analysts find and address security threats is Logpoint Converged SIEM. It identifies anomalous user behavior, allowing for rapid analysis, and provides pre-defined alert criteria covering Tactics, Techniques, and Procedures (TTPs). By automating the investigation and incident response, Logpoint SOAR accelerates the time to diagnosis and repair (TDIR) by coordinating hardware, software, and alarms from multiple sources and systems. To identify insider threats, UEBA looks for unusual activity from insiders. The native endpoint agent, AgentX, makes sure that actions like isolating compromised endpoints are taken in real-time.

AgentX gives Converged SIEM EDR features in addition to SIEM and SOAR. Using out-of-the-box alerts, threat intelligence, orchestration and automation actions that expedite manual processes and respond to and remediate incidents, such a security operations platform enables organizations to quickly detect and respond to various assaults.

3.CVE-2011-2523

2.1 Introduction

A very significant vulnerability has been discovered in vsftpd 2.3. 4 (File Transfer Software). An unidentified code block of the component Service Port 6200 is vulnerable to this flaw. There is a vulnerability for OS command injection due to manipulation with an unknown input.

3.2 Methodology

Version 2.3.4 of the vsftpd FTP server has a backdoor due to this CVE. A backdoored version was posted to the main website that hosted the client that could be downloaded. The backdoor operates by first determining whether the username string ends in ":)"; if so, it invokes vsf_sysutil_extra(). After binding to port 6200, the called function waits for a connection. After then, any command sent to that port is carried out by execl.

Even though it could be alluring to take advantage of the flaw in order to win quickly, doing so has certain unintended risks. The backdoor and FTP use unencrypted protocols to function. As a result, any attacker with access to the same data that you did might intercept a Wireshark trace of your exploit.

We can avoid this danger from:

When utilizing Metasploit for backdoor exploits, the reverse_openssl payload should be taken into account.

When utilizing an exploit script, think about initiating a Metasploit handler and subsequently updating it to a Meterpreter shell. By default, Meterpreter is encrypted.

Conclusion

When there are public reports and PoCs, use those via CVE analysis increase my understanding about the vulnerability and try to understand the root cause. Don't take the report as final though, as code is ever changing. Also, might be able to see a bit further that the researcher writing the report, or understand ways in which a patch might have not fixed the root cause. This can lead to discovery of new vulnerabilities or variants.

References

[1] "What is EternalBlue? | Security Encyclopedia," What is EternalBlue? | Security Encyclopedia. https://www.hypr.com/security-encyclopedia/eternalblue (accessed Dec. 06, 2022).

THANK YOU