SLIIT

Discover Your Future

Systems and Network Programming - IE2012

YEAR 2 , SEMESTER 1

CVE RESEARCH REPORT 1

IT22315496

Chamod Anuradha

1) Contents

Abstract

In today's networked digital environment, remote code execution (RCE) is a serious security risk. This abstract gives a general overview of RCE, emphasizing its definition, possible hazards, underlying vulnerabilities, and practical mitigation techniques.

RCE is the term used to describe the malevolent capacity to run instructions or arbitrary code on a remote system or application. Data integrity, confidentiality, and system operation are seriously threatened by attackers who take advantage of weaknesses in target systems to get unauthorized access and control. Injection attacks, in which adversaries alter user inputs or data channels to insert malicious code payloads, are often used in RCE.

The significance of proactive security measures is emphasized in this abstract. In order to mitigate RCE attacks, it addresses the vital roles that vulnerability assessment, secure coding techniques, and prompt patch management play. Strict access restrictions, intrusion detection systems, and web application firewalls are emphasized as essential defensive techniques.

Organizations and people alike must be aware of the dangers associated with RCE attacks sincesuccessful assaults may lead to data breaches, system compromises, and legal repercussions forthe attackers. Maintaining vigilance and putting strong security measures in place are critical to preventing Remote Code Execution attacks as technology advances.

Introduction

Cybersecurity is a constantly changing concern in an age characterized by the fast growth of technology and the pervasive integration of digital systems into every part of our lives. The continuous expansion of linked networks and the widespread use of software applications expose people and businesses to a growing variety of risks. It is critical to recognize and comprehend software and hardware system vulnerabilities in order to remedy these issues.

The vital area of Common Vulnerabilities and Exposures (CVE) research is explored in this study. A widely accepted and defined method for classifying and monitoring vulnerabilities in hardware and software components is called CVE. The fundamental building blocks for comprehending, recording, and reducing cybersecurity risks are contained in CVE entries.

Vulnerabilities are found at an alarming pace as the digital world keeps growing. Organizations, governmental bodies, and people are all at significant risk from cyberattacks, data breaches, and their aftermath. The cybersecurity community relies heavily on CVE, a comprehensive catalog of known vulnerabilities. Through the provision of a methodical and widely accepted approach to detecting and characterizing vulnerabilities, CVE enables professionals, researchers, and stakeholders to communicate, work together, and develop efficient mitigation techniques.

CVE Research Topic

- Remote Code Execution

Introduction

An attack known as remote code execution (RCE) happens when an attacker may run arbitrary code or instructions on a target system or application from a distance. assaults of this kind have the potential to be very dangerous since they provide the attacker with the ability to take over asystem, steal confidential information, alter the way the system behaves, and even use it as a springboard for further assaults.

TryHackMe box link - tryhackme.com/jr/cveresearchproject

An overview of the main ideas behind remote code execution is provided

Remote Attack Vector:

- Since remote code execution (RCE) attacks are usually conducted remotely, the attacker does not need physical access to the target machine. Attackers often take advantage of flaws in services or software that are available across a network, including servers, networked devices, and online applications.

Vulnerabilities:

- RCE attacks often rely on the presence of system or software vulnerabilities. RCE is often caused by vulnerabilities like as buffer overflows, input validation mistakes, and improper deserialization.

Injection Attacks:

- Injection attacks, such SQL injection and command injection, are a popular means of achieving RCE. In order to carry out these attacks, malicious code or instructions are injected into user inputs or other data channels that the target system processes.

Exploitation:

- An attacker must locate and take advantage of a vulnerability in the target system in order to launch an RCE attack. This might include transmitting carefully constructed payloads or inputs that cause the vulnerability and let the attacker run their code.

Payloads:

- Payloads, which are bits of code or instructions intended to take advantage of a vulnerability and run arbitrary code on the target system, are often used by attackers in RCE attacks. These payloads have been thoughtfully designed to exploit a particular vulnerability.

Consequences:

- An attacker may be able to carry out any action authorized by the compromised system or application after they have obtained RCE. This covers data theft, file alteration or deletion, malware or backdoor installation, and system takeover.

Mitigation:

- Organizations and developers should adhere to security best practices, such as input validation, code reviews, and the timely patching of known vulnerabilities, in order to avoid RCE attacks. RCE attempts may also be found and stopped with the use of intrusion detection systems and web application firewalls.

Common Targets:

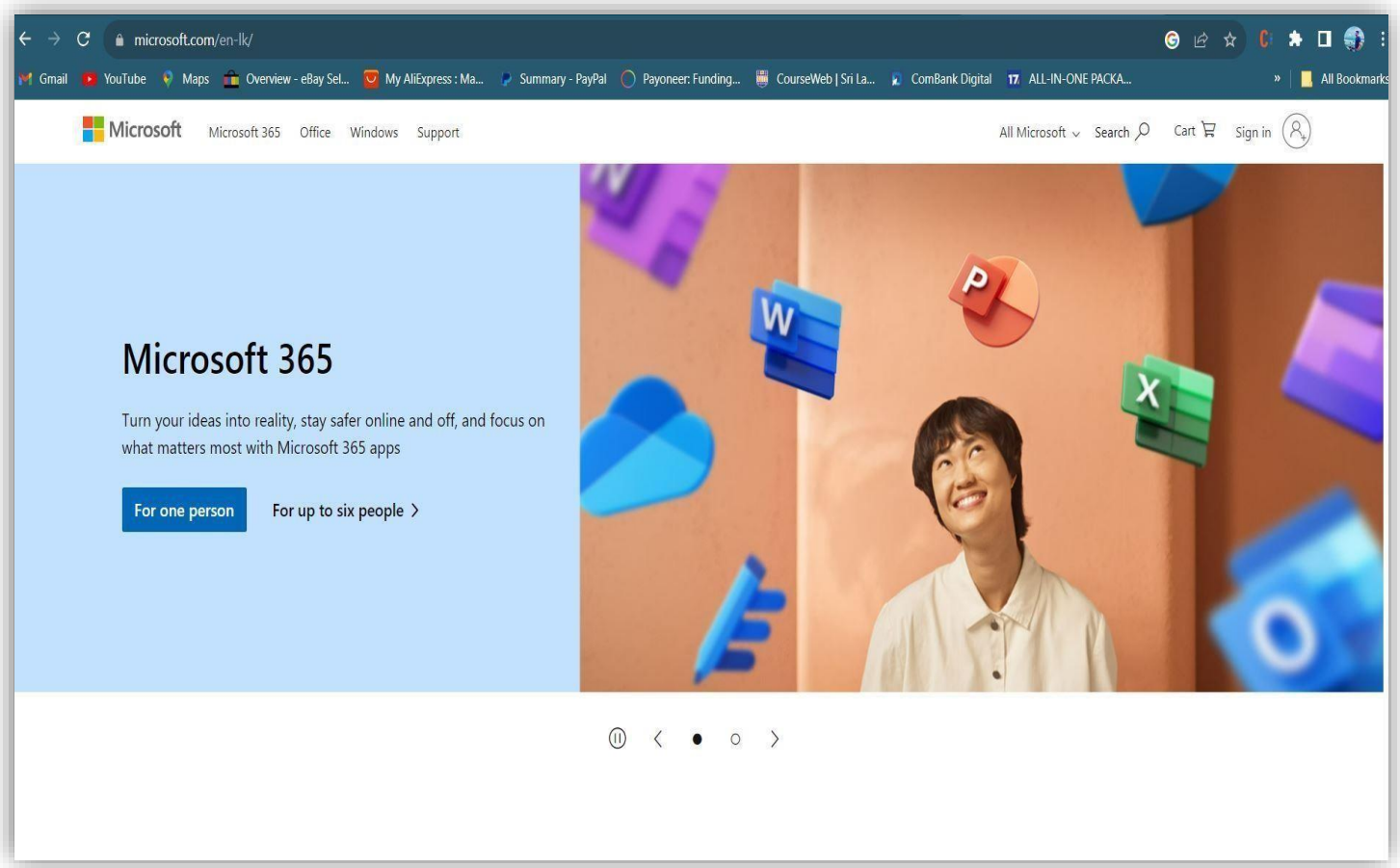
- Common targets of RCE attacks include servers, online apps, Internet of Things devices, and any networked system. Online apps are especially vulnerable because of the complexity of web technology and the variety of user inputs they might process.

Legal Implications:

- RCE assaults are prohibited and may have serious legal repercussions for those who carry them out. Prison time and fines are possible punishments, depending on the jurisdiction and degree of harm.

Research Findings

CVE-2021- 26855 (ProxyLogon)



"ProxyLogon," also known as CVE-2021-26855, is a significant security flaw that impacts Microsoft Exchange Server, a popular email and collaboration tool. Early in 2021, this vulnerability was found, and because of its potential for mass exploitation, it attracted a lot of attention. Please be aware that the situation may have changed after September 2021, and my understanding is based on information that was accessible at that time.

Introduction:

Microsoft Exchange Server was impacted by a major security vulnerability known as ProxyLogon, or CVE-2021-26855. When it was first revealed in early 2021, its potential for broad exploitation attracted a lot of interest. A server-side request forgery (SSRF) vulnerabilityexisted.

Impact of the Vulnerability: CVE-2021-26855 (ProxyLogon)

1. Server Compromise: Attackers may have been able to compromise the Exchange Server by sending arbitrary HTTP requests to it by taking advantage of this vulnerability.

2. Remote Code Execution: If the SSRF is successfully exploited, attackers may be able to take complete control of the Exchange Server via remote code execution.

3. Unauthorized Access: Attackers could enter the server without authorization, perhaps jeopardizing user accounts, private email correspondence, and other data.

4. Data Exfiltration: With this access, hackers could be able to take private information from the hacked server by stealing emails and other data.

Vulnerability Summary:

CVE-2021-26855 Microsoft Exchange Server has a server-side request forgery (SSRF) vulnerability called ProxyLogin. Attackers might potentially breach the server, execute code remotely, gain unauthorized access, and exfiltrate data by sending arbitrary HTTP requests to the server.

Potential Countermeasures:

The following steps were recommended for organizations and administrators to take in orderto reduce the risks related to CVE-2021-26855 (ProxyLogon):

1. Patch and Update: To fix this vulnerability, apply the security updates that Microsoft has published. Patching Exchange Servers on time is essential for their security.

2. Scan for Indicators of Compromise (IOCs): Make use of Microsoft and security vendor technologies to search Exchange Servers for indications of compromise.

3. Verify Unauthorized Entry: Examine the logs to see if there are any instances of illegal access or data espionage. Examine impacted accounts and make sure they are secure.

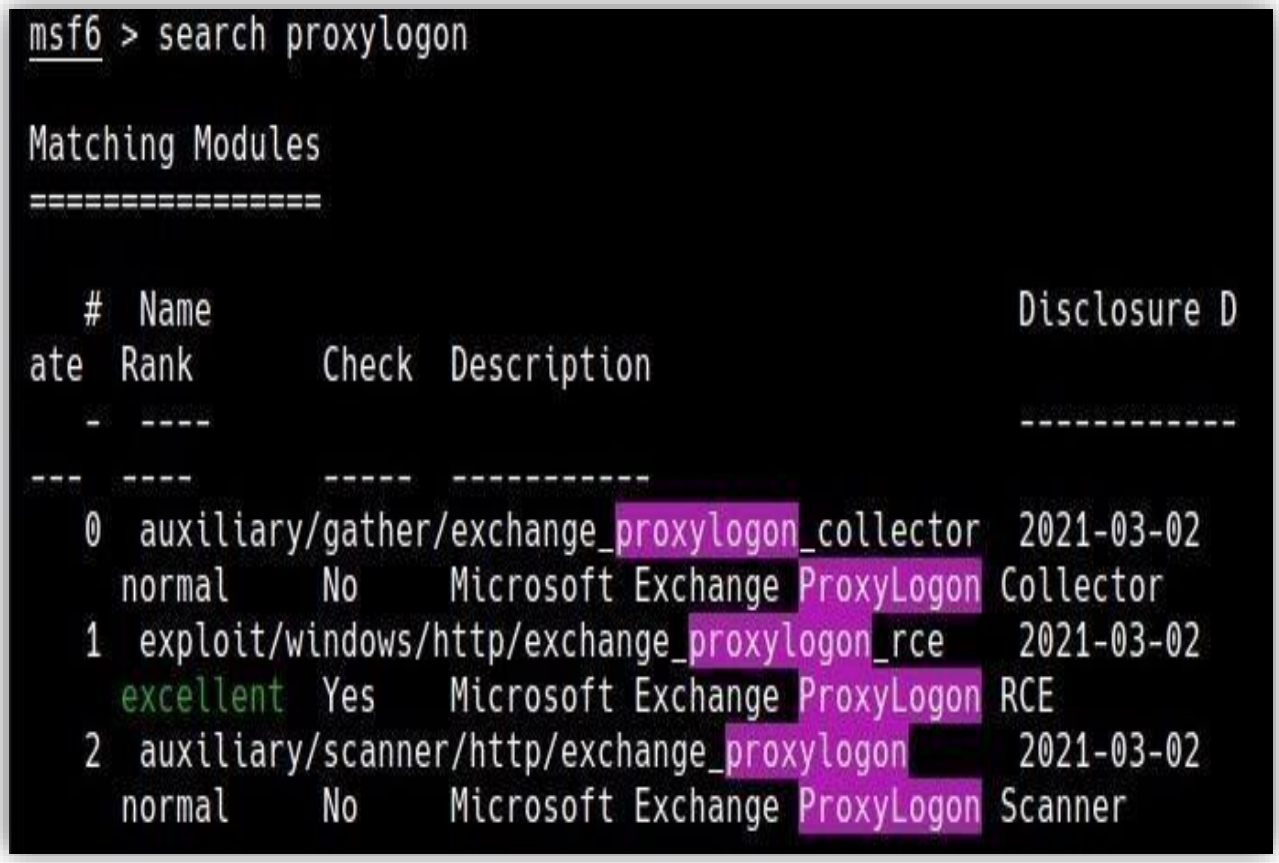
4. Implement Security Best Practices : Adhere to recommended setup guidelines for Exchange Server, which include limiting external exposure, requiring robust authentication, and limiting superfluous permissions.

5. Monitor for strange behavior: Keep an eye out for any strange behavior or indications of exploitation by continuously monitoring system logs and network traffic.

6. Educate Users: Inform users and staff members of the potential uses of social engineering and phishing techniques by attackers to access Exchange servers.

Detect proxy login vulnerability

There are modules in Metasploit that address these issues. Let us use these modules.



uses the CVE-2021-26855 vulnerability to its advantage and dumps all of the mailboxcontents.

```
msf6 > use 0
msf6 auxiliary(gather/exchange_proxylogon_collector) > show option
s

Module options (auxiliary/gather/exchange_proxylogon_collector):

   Name         Current Settin  Required  Description
                g
   ----         --------------  --------  -----------
   ATTACHMENTS  true            yes       Dump documents attache
                                          d to an email
   EMAIL                        yes       The email account what
                                           you want dump
   FOLDER       inbox           yes       The email folder what
                                          you want dump
   METHOD       POST            yes       HTTP Method to use for
                                           the check (only). (Ac
```

vulnerability to acquire admin access without authentication. It then uses the CVE-2021-27065 vulnerability to write any file to the target in order to accomplish remote code execution. By default, every version listed above is susceptible.

```
msf6 > use 1
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/http/exchange_proxylogon_rce) > show oprions
[-] Invalid parameter "oprions", use "show -h" for more informatio
n
msf6 exploit(windows/http/exchange_proxylogon_rce) > show options

Module options (exploit/windows/http/exchange_proxylogon_rce):

   Name          Current Settin  Required  Description
                 g
   ----          --------------  --------  -----------
   EMAIL                         yes       A known email addres
                                           s for this organizat
                                           ion
   METHOD        POST            yes       HTTP Method to use f
                                           or the check (Accept
```

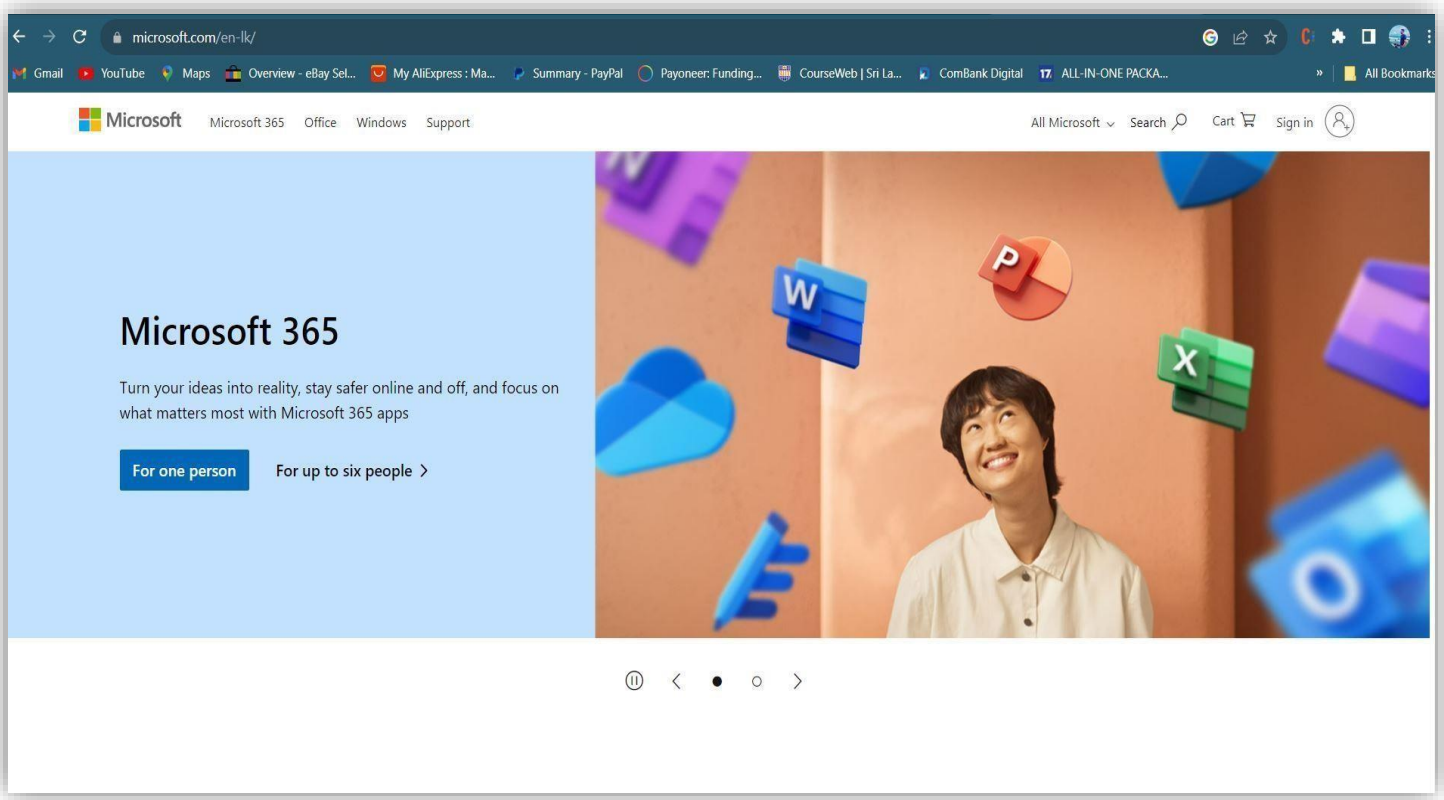
check for the Exchange Server vulnerability known as CVE-2021-26855.

```
msf6 > use 2
msf6 auxiliary(scanner/http/exchange_proxylogon) > show options

Module options (auxiliary/scanner/http/exchange_proxylogon):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   METHOD   POST             yes       HTTP Method to use for th
                                       e check. (Accepted: GET,
                                       POST)
   Proxies                   no        A proxy chain of format t
                                       ype:host:port[,type:host:
                                       port][...]
   RHOSTS                    yes       The target host(s), range
                                        CIDR identifier, or host
                                       s file with syntax 'file:
                                       <path>'
   RPORT    443              yes       The target port (TCP)
```

CVE-2021- 27065 (ProxyLogon)



An important security flaw in Microsoft Exchange Server was identified in early 2021 under the CVE-2021-27065, often known as ProxyLogon. Given its potential for broad exploitation by malevolent actors, this vulnerability garnered a great deal of attention. The investigation on CVE-2021-27065 yielded the following major conclusions.

Summary of Vulnerabilities:

CVE-2021-27065 is a component of the ProxyLogon group of four related vulnerabilities. The precise vulnerability in question is a Microsoft Exchange Server unauthenticated remote code execution bug.
Exchange Server 2013, 2016, and 2019 are among the on-premises versions of MicrosoftExchange Server that are predominantly impacted.
The flaw gave hackers the ability to run any code on the Exchange Server without requiringauthentication, which may have resulted in the system's total infiltration.

Impact of the Vulnerabilities:

Attackers might be able to: Get unauthorized access to the Exchange Server by taking advantageof this vulnerability.
Pilfer private information, including user passwords, emails, and other sensitive data. Put malware or ransomware onto the server that has been hacked.
Progression across the network and the escalation of privileges might result in a more extensivebreach of the company's IT system.

Potential Mitigations:

Microsoft fixed the ProxyLogon vulnerabilities by releasing security upgrades. Using these fixesright now is essential if you want to keep your Exchange Server safe.
If patching cannot be completed right away, Microsoft has a set of temporary mitigations thatmay assist lower the risk of exploitation. Among them are: Rolling out a security patch.
Limiting unauthorized access to the Exchange server.
using intrusion detection/prevention systems to stop known attack patterns. looking for signs of compromise on your network to find any possible security hole

Importance of Timely Patching:

Soon after it was disclosed, threat actors began aggressively using CVE-2021-27065 inthe wild,which attracted a lot of attention. This emphasizes how crucial it is toimplement security updates for serious vulnerabilities as soon as possible.

Organizations that put off patching may be left vulnerable to serious dangers because hackersmight quickly take advantage of vulnerabilities that are already known.

Conclusion

In summary, the Common Vulnerabilities and Exposures (CVE) system is a critical tool used by the cybersecurity community to manage the constantly evolving world of digital threats. CVE is a fundamental tool that helps academics, businesses, and cybersecurity professionals prioritize vulnerabilities, communicate clearly, and create plans to protect important systems and data. In this age of unrelenting technological development, the importance of CVE research is immeasurable. By keeping up a thorough awareness of vulnerabilities, their effects, and mitigation techniques, we may better guard our globalized society from the always changing threats posed by cybersecurity.


THANK YOU!