Windows Domain Name System (DNS) server remote code (SIGRed Vulnerability)

[CVE– 2020- 1350]

12th of May 2021

Secure Software System | Assignment 01

Jayasundara H. M. D. E. K. | IT 19081762

Email: it19081762@my.sliit.lk

ABSTRACT

On 14th July 2020 in United States , Microsoft acknowledged a critical remote code execution vulnerability (CVE – 2020 - 1350) existing in Windows Domain Name System (DNS) when it fails to properly handle requests. An adversary who successfully exploits the vulnerability could run arbitrary code or malicious code in the context of the Local System Account. And this vulnerability rests on the DNS client while it handles specific requests. This means that an attacker who does not perform an authentication can gain control of an account that exists locally on the system, even remotely. This will allow the host to reach a complete compromise. The nature of the attack is to turn this vulnerability into worms among the affected DNS servers. It will then become part of the core networking of the Windows DNS server. In most cases these systems, which run on domain controllers, need to be constantly updated. Considering the potential impact and the criticality of insecurity, none of its exploits have yet been properly articulated, and these exploits are on the rise. Microsoft has pointed out that patching is not the only option, although minor changes to essential registrars may have minor side effects. Microsoft continues to update a large number of CVEs.

Keywords: *Common Vulnerabilities and Exposures (CVE), SIGRed vulnerability, Common Vulnerability Scoring System* (*CVSS), User Datagram Protocol (UDP), Transmission Control Protocol (TCP)*

1. INTRODUCTION

DNS is translating a user-friendly computer hostnames into IP addresses, known as the "Internet Phone Book". It is a network protocol. DNS servers are considered to be an integral part of the Internet and have many solutions and implementations. But only a few of those methods are widely used. The Windows DNS server is a server implemented by Microsoft Organization. It can also be considered as an essential component of the Windows domain environment. SIGRed (CVE-2020-1350) is a critical version of the Windows Domain Name System (DNS) server that affected the Windows server versions from year 2003 to 2019. The basic value of CVSS is 10. Since that value is activated on a SYSTEM by a service or service that triggers a malicious DNS response, if it is successfully exploited by an attacker, that attacker will be granted domain administrator rights. [3]

2. OVERVIEW

DNS basically uses the 53rd port of user datagram protocol (UDP), to fulfill the requests. Domain name system Inquiries consist of one reply from the server followed by one protocol request. Converting names to Internet Protocol addresses, domain name system also serves other purposes.

For example, mail exchangers use Domain Name System to find the perfect mail server for email delivery.

- Domain Name System (DNS) operates over User Datagram Protocol / Transmission Control Protocol port 53.
- A single Domain Name System response or a query is limited to 4,096 bits in User Datagram Protocol (UDP) and the 64 KB in Transmission Control Protocol.
- Domain name system is decentralized and hierarchal in nature. Meaning of that is when a Domain Name System (DNS) server does not know the correct answer to a query it receives.
- Top of the hierarchy there are 13 of root domain name system servers in world. [1]

The domain name system client and the server are implemented in two different modules in Windows. They are:

2.1 **Domain Name System Client –** dnsapi.dll is a file associated with API components for DNS clients included in Windows. It does not cause any harm to a computer. In fact, it is used to solve DNS clients. This dnsapi.dll also stores the settings needed to configure domain name system (DNS)

configurations from Microsoft-Windows-DNS-client included components.

2.2 **Domain Name System Server –** Windows servers use the dns.exe service for network domain requests for a domain name system, and dns.exe is responsible for answering DNS queries that establish the role of the Windows server DNS.

For example, the conversion function (127.0. 0.5) of a localhost computer uses DNS requests to communicate over a network.

3. STATEMENT / OBJECTIVES OF THE RESEARCH

When Windows domain name system servers is failing to handle the users' requests properly, it runs the risk of executing remote code under the code name "SIGRed". An attacker who successfully understands the vulnerability and exploits it will be able to run arbitrary codes or malicious codes in the context of the local system account. For Windows servers that are configured as domain name system servers, this risk is even higher. A malicious actor or a hacker who has not been authenticated sends malicious requests to the Windows domain name system server to exploit the vulnerability and changing the way these Windows DNS servers handle requests could also jeopardize the update. This report focuses on the vulnerabilities of these Windows DNS servers and how to identify them. As the risk is very high, it is also mentioned here how to take action to protect against this.

4. SCENARIO

CVE-2020-1350 means that for an exploitative and threatening actor, access to a malicious DNS server requires a DNS server found within an organization. Domain management is found by adding a name server (NS) record that specifies which DNS server is being managed. This domain is authorized by a malicious DNS server. For example: using methods such as phishing tricks to click and trick users into using a malicious DNS server to troubleshoot that domain and trigger a link to the infected DNS server. After the victim's DNS server inquiries about the malicious DNS server, it can begin to respond to malicious payments and threats to threatening actors.

5. PREPARING THE ENVIRONMENT

There are two major types of study aids. The first query is an error in the way the DNS server interprets it, and the second is an error in the way the domain name system server interprets a response to a forwarded query.

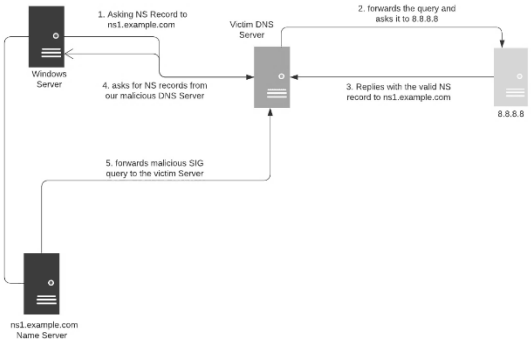
There is no complex structure for DNS queries. Therefore, the chances of finding problems in the analysis are low. For that reason, we had to focus on tasks that analyze the responses to future queries. A query refers to the ability to use DNS architecture to answer unanswered queries.

Number of network environments configure the forward to well-known domain name system servers such as Google [8.8.8.8] or Cloudflare [1.1.1.1]. A server that is not under the control of a malicious actor is used.

This means that although it is possible to find a problem in interpreting Domain Name System (DNS) responses, an intermediary must be created to exploit it. Certainly, it will not be enough.

6. THE VULNERABILITY CVE – 2020 – 1350

This risk has been identified as CVE-2020-1350 and is assigned a CVSS basis of 10 points. Risk is considered a 'worm' because it has potential. This potential allows it to spread among vulnerable devices without user interaction.



As DNS is widely installed, this risk exploitation on domain controllers can have a significant impact on corporate networks and services. Microsoft has advised that there are no mitigations for this risk, and that the only possible course of action is to apply security patches. For organizations that are

unable to apply quickly, Microsoft has provided a patch application and a registry modification program.

When replying to a long SIG report, the DNS server is at risk of being misled by inquiries due to the repetitive nature of the malicious domain name system. Due to the specifics of the DNS, the transport protocol used for DNS is exploited at its risk level by using TCP instead of UDP. An attacker gains domain administrator privileges when its vulnerability is exploited, allowing it to build network infrastructure. In most cases DNS servers will also be domain administrators. Find out more about the vulnerability and its exploitation. This vulnerability has been identified by Microsoft as a worm, which means that the spread of a stimulus occurs without any human interaction. Also, any malicious software used from the moment of its release will be properly understood.

6.1 AFFECTED VERSIONS

Windows Server Installation Configured as domain name system (DNS) Servers an attacker or a hacker has the ability to run malicious code in the context of the local system account of these vulnerable clients while running Windows Server 2008. This vulnerability affects both the server core and the full installation of the Windows server, and the recently released version of Windows Server 20H2 is also at risk. Failure to run the Microsoft DNS server may result in insecurity and the potential for a protocol-level error to occur. Therefore, it was discovered that this does not affect to any other non-Microsoft domain name system server activations. If an organization uses not only existing domain controllers but also Infoblox for DNS, this risk will not directly affect the domain administrators of that organization.

Servers at risk include the following windows servers:

- Windows server 2008 for 32-bit systems service pack 2 and server sore installation
- Windows server 2008 for X64-based systems service pack 2 and server core installation
- Windows server 2008 for X64-based system service pack 1 and server sore installation
- Windows server 2012 and server core installation
- Windows server 2012 R2 and server core installation
- Windows server 2016 and server core installation
- Windows server 2019 and server core installation
- Windows server version 1909, version 1903, and version 2004 (server core installation)

7. TECHNICAL ANALYSIS

RR_AllocateEx API size parameters are expected to be 16 bits. For that reason, it can be considered as the primary reason for the existence of this error. It is safe to assume that the size of a single domain name system message does not exceed 64KB on average. Therefore, this behavior cannot be presented as a problem. However, when calculating the size of a buffer, the result of *Name_PacketNameToCountNameEx* Be careful and this assumption is wrong when it comes to consideration. This happens when calculating the effective size of the compressed name with the corresponding function in *Name_PacketNameToCountNameEx*, which does not specify the number of bytes used to represent the package.

8. WORKAROUND

Transmission Control Protocol-based (TCP) domain name system response packets that exceed the recommended values are left blank without error, which increases the likelihood that some queries will go unanswered. It is likely to be the root cause of unexpected failures. This functionality will only be negatively affected if a DNS server receives validated TCP responses that allow more than 65,280 bytes to minimize it. Reduced values are not directly affected by standard applications or recurring queries, and there may be a non-standard usage case in a given environment. In order to determine the possible adverse effects of activating clients for that functionality, it is advisable to enable the diagnostic logging methodology. It is best to review a log file to identify and verify the presence of abnormally large TCP response packets, capturing a sample set representing the typical business.

On Windows PowerShell, if you want to add registry values using the following lines and run them with the help of a Windows PowerShell window, you need to restart the DNS server.

$ RegPath = "HKLM: \ SYSTEM \ CurrentControlSet \ Services \ DNS \ Parameters"

New-ItemProperty -Path $ RegPath -Name TcpReceivePacketSize -Value 0xFF00 -PropertyType DWORD

Restart-Service DNS

The following lines on the Windows PowerShell should continue to run in a tall Windows PowerShell window, even after applying the update to flip the temporary registry keys.

$ RegPath = "HKLM: \ SYSTEM \ CurrentControlSet \ Services \ DNS \ Parameters"

Remove-ItemProperty -Path $ RegPath -Name TcpReceivePacketSize

Restart-Service DNS

9. DETECTION

Remote code activation refers to the ability of a hacker or a malicious actor to gain access to another computer device and to change the location of the device geographically from one location to another. The best way to protect computer devices from the risk of remote code activation is to install holes that allow the attacker to gain access.

Windows domain name system (DNS) servers run the risk of executing remote code, and any attacker who successfully exploits that vulnerability may be able to run arbitrary code across the network in the context of a local system account.

There are no specific access conditions or expulsion conditions, and an attacker can expect success again against vulnerable components. The hacker or a malicious actor is unauthorized and therefore does not need access to any settings or files to carry out the attack. Only resources managed by the same security authority can be vulnerable to an exploitative risk, while the vulnerable components and the affected components are in the same situation. Or both are managed by the same security authority.

Confidentiality, Integrity, and Availability (CIA tried) are all three of the highest risk factors. The secrecy of this vulnerable situation has been completely lost. As a result of that loss, all the resources in the affected components are exposed to the attacker. Alternatively, access to only a limited amount of information can have a direct and serious impact on the information that is detected. Similarly, a complete loss of integrity or a loss of a completely safe state can be seen. For example, an attacker can completely or partially modify or delete any number of files made to protect the affected component. Similarly, a complete loss of integrity or a loss of a completely safe state can be seen. For example, an attacker can completely or partially modify or delete any number of files made to protect the affected component. Availability of this windows domain name system (DNS) remote code execution (RCE) vulnerability is completely lost. As a result, the attacker has the opportunity to completely deny access to the resources of all affected components. The attacker has the ability to continue attacking and therefore the loss may continue. Otherwise, the situation is likely to continue after the attack. Alternatively, you can see the possibility for an attacker to deny any utility. But can have direct severity consequences for components that have been subjected to unavailable effects. For example, an attacker's attack does not completely destroy all existing connections, and attacks are used to prevent new connections. That is, for a completely successful attack, only a very small amount of memory may be leaked, but after continuous exploitation it may not be possible to fully obtain the required services.

9.1 MODERATE DETECTION DIFFICULTY

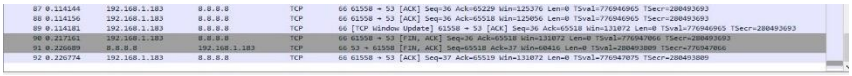
Many products like EDR(Endpoint Detection and Response), proxy servers, and firewalls fail to detect this vulnerability and the attack. In addition to that, Windows-based login tools do not display specific error codes. Network-based detection is one of the most effective ways to identify this threat.

9.2 DETECTION: NETWORK BASED

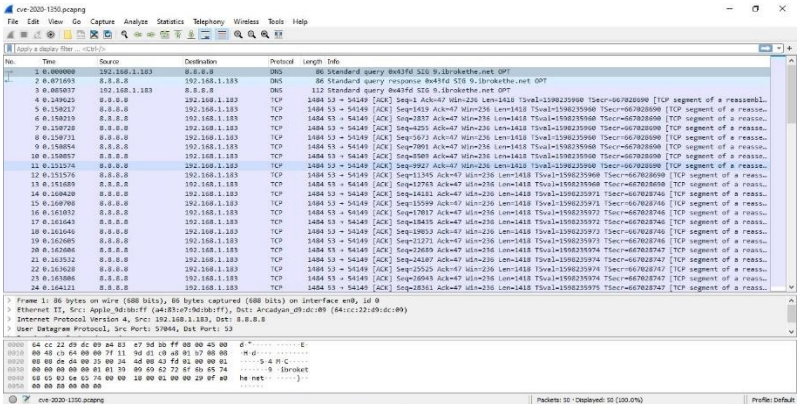
Ingredients that are considered vulnerable are bound to the store in the network. Attacker kits are listed, but it extends beyond other options. Such a risk is known as 'remote exploitation'. Using one or more network hoops, for example: using one or more routers, can be considered a protocol-level exploitative attack.

10. TRIGER THE VULNERABILITY

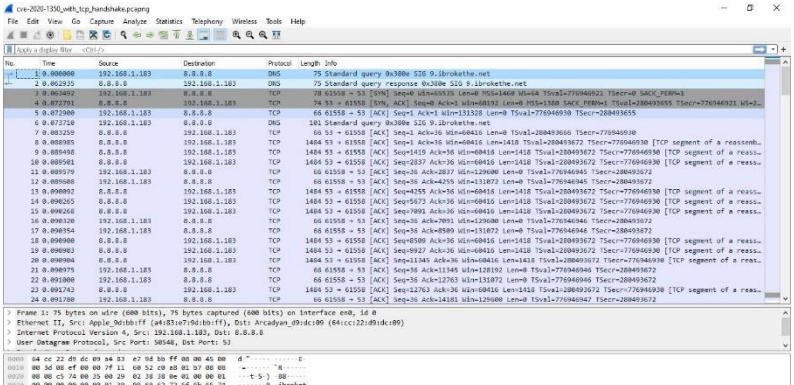
A malicious DNS server can make specific inquiries to a malicious DNS client and respond to malicious responses when they are matched in order. All that is needed to trigger this vulnerability is for the victim domain name system client to request an SIG report and to respond to an SIG response of length >= 64KB with a long signature. The size of the DNS is limited to 512 bytes, which is higher than the UDP. And if the EDNS0 server is supported, it would be about 4,096 bytes. But in any case, it will not be enough to trigger a risk.



11. EXPLOITATION



Hope to present a brief summary of how it works. It is first triggered by a DNS request for a malicious domain on the LAN. It is more specific and requests for SIG records. For example: “evil_domain.com”.



The received request included in the vulnerable Windows server is sent to the DNS server, which in turn makes a request to any DNS requesting that vulnerable client. This is usually done with a standard Google IP. That is, Google DNS responds with servers whose names are for the malicious domain. The vulnerable client then acts as a DNS server and sends a request to the malicious domain name system server. The malicious client then responds with 2 bytes full and the remaining payment. In this case, the provision is smaller than the required amount. Eventually the Domain Name System (DNS) server included in the vulnerable server crashes.

11.1 EXPLOIT CODE MATURISTY

This metric calculates the probability of being at risk, and the measured value is generally based on current exploitation methods. Acquiring codes basically requires skill and experience and using that experience can lead to exploitation or active-internal exploitation. There is code to exploit the concept of this windows DNS remote code execution vulnerability. Otherwise, an attack representation would not be practical for these systems. This exploit code or technical methodology does not always work and may require significant modification if exploited by an experienced and skilled attacker. [15] [16]

11.2 RECOMANDATION LEVEL

Risk levels of risk are an important factor for priority, and it is not possible to identify a normal risk level at the time of first disclosure. Workflows or Hotfix will provide missing treatments until a patch is officially applied or an upgrade is issued. Temporary scores are adjusted to lower levels for each stage, reflecting the reduced emergencies at the end of treatment. There is an official solution / complete sales solution to this risk. Microsoft has released an official patch here. When not, an improvement is made. [15] [16]

11.3 REPORT CONFIDECE

This section emphasizes the reliability of technical information and the existence of risk, and in some cases only the existence of insecurity. But in the absence of specific information, it can sometimes be difficult to point it out.

For example: identified as unsuitable for impact but the root cause is unknown.

Although the research is not at a definite level, the risk status is subsequently confirmed by the use of research that suggests potential risk factors. Finally, acknowledgments made by the author or seller of the affected technology can confirm insecurity. When there is a definite risk for this insecurity, the risk of an emergency will also increase. This confirms that the Windows DNS RCE vulnerability is at the highest level of risk. There are detailed reports for this and there is a possibility of active reproductions. That is, it provides active exploitation. Source codes can be used to independently verify research statements. Otherwise, the author or seller of the affected codes will make a full confirmation of the insecurity. [15] [16]

11.4 EXECUTION

To trigger a Windows Domain Name System (DNS) server vulnerability, run *nslookup -type=sig 9.your_domain_name_here dns_server_to_target,* where '9' is the subdomain. It is really needed here and will deal with the use of the script so there will be no need to modify the domain records in any way.

For example: it is advisable to run *nslookup -type = sig 9.ibrokethe.net 127.0.0.1* while running this server.

12. PREVENTION METHODS

The patch issued by Microsoft must be installed without delay. The Cyber Infrastructure Security Agency (CISA), under the Department of Homeland Security in U.S., issued an order on 16th of July last year, giving U.S. federal agencies about a day to reduce this risk. Microsoft has officially introduced a registry-based program to protect against this vulnerability for clients who are largely in critical infrastructure and cannot be patched. This functionality also limits the number of packets used for the largest TCP-based DNS responses permitted. By changing the registry key below, will be able to apply it and reboot the system.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters

DWORD = TcpReceivePacketSize

Value = 0xFF00

The invasion prevention system and the vulnerability system help to take advantage of the vulnerabilities in the application to try to capture it or prevent it and protect it from exploitation competition from the threat of crash. Checkpoints in the next generation of firewalls are set to automatically update IPS security. Whether the risk was released a few years ago or a few minutes ago, the organization is able to defend itself.

At present, the security at its extreme point must be considered as a critical role in the activation of the remote workforce. Harmony Endpoint provides security for a wide range of endpoints with the highest level of security. Harmony Endpoint also detects the behavior of ransomware, such as file-encryption and attempts to disable backups on an operating system. It also automatically replaces files that are encrypted in ransomware.

13. CONCLUSIONS

This seriousness is recognized by Microsoft as a high level of seriousness and was given the name CVE-2020-1350 vulnerability. I also believe that the probability of exploiting this risk is high as all the primaries required to exploit this error have been found internally. Due to time constraints, I did not continue to exploit the bug.

But it also involves tying together all the primitives of exploitation. I believe a determined attacker will be able to exploit it. In many cases unsuitable Windows domain environments, especially domain controllers, can be found, and the successful exploitation of this risk has a severe impact. In addition, some Internet Service Providers (ISPs) configure their public DNS servers as WinDNS.

To prevent this risk exploitation, I recommend pasting the affected Windows DNS servers from Internet service providers.

As a temporary solution, it is advisable to set the maximum length of a DNS message passing through TCP to 0xFF00 until a patch is applied. This can eliminate the risk to some extent.

14. EXCLUSIVE SUMMARY

Existing versions of Microsoft Windows Server from 2003 to Windows Microsoft Server 2019 (CVE: 2020-1350) include a number of security vulnerabilities regarding Microsoft DNS server activation risks. Microsoft has given CVSS a 10-point rating for this vulnerability because it indicates a very serious error. Successful exploitation is fully integrated into the directory environment, enabling domain controller (DC) remote code implementation and (RCE)

integration into the entire network. All the machines in the non-consensual domain are endangered and this article will show you how to successfully exploit this vulnerable situation which is about 5 months old. It therefore outlines all the facts, including how to create the environment needed for this exploitative situation to work, that is, how to hunt down this threat. [16]

Severity of the vulnerability	**10**
Common Vulnerability Scoring System (CVSS)	(AV:N/AC:L/Au:N/C:C/I:C/A:C)
Date of published	03/09/2021
Date of created	03/10/2021
Date of added	03/09/2021
Date of modified	03/22/2021

15. FUTURE RESEARCH

The implementation of remote codes has become one of the most important issues at present, as the analysis is based on the relevant activities as indicated by the clauses in this report. Based on the study, gaps can be further suggested and improved on its basis. It is also possible to develop models related to the future environment. It makes it easier to handle situations like an efficient mechanism.

AKNOWLADGMENT

First of all, I would like to pay tribute to Mr. Lakmal Rupasinghe, senior lecturer in Sr Lanka Institute of Information Technology (SLIIT) and Miss Chethana Liyanapathirana, lectures in Secure Software System (SSS) at the university. for their efforts to expand our knowledge through the focus of study on a new topic. We consider it a great privilege to be able to enhance our knowledge through a wide range of valuable information in new dimensions while reviewing the research project. I would also like to express my appreciation to all my colleagues who have contributed to my research. I was able to do this research better and look at the research in new dimensions. I will never forget the support of my family members and I would like to express my gratitude for that.

Also, I would like to thank my university for improving my education. I would like to pay my respects for leading the way to conquer the world by producing thousands like me. I look forward to doing this with my 100% commitment and full effort for any assignment given. Finally, I would like to express my appreciation for all the projects and research that led to the results presented in this article and helped make this project a success.

REFERENCES

[1] A. Viklund, "CVE-2020-1350 - Windows DNS Server Vulnerability - SIGRed," 2020 July 16.

[2] "Windows DNS Server Remote Code Execution Vulnerability," Microsoft, 14 July 2020. [Online]. Available: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1350.

[3] "CVE-2020-1350," CVE, [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1350.

[4] akb_intel_feed_importer, "CVE-2020-1350 Windows DNS Server Remote Code Execution (SigRed)," 14 July 2020. [Online]. Available: https://attackerkb.com/topics/egp32neD6z/cve-2020-1350-windows-dns-server-remote-code-execution-sigred#vuln-details.

[5] C. Admin, "Vulnerability in Microsoft Windows Server," Sri Lanka CERT, 16 July 2020. [Online]. Available: https://www.cert.gov.lk/view?lang=en&articleID=12.

[6] E. Kost, "Critical Microsoft Exchange flaw: What is CVE-2021-26855?," UpGuard, 25 May 2021. [Online]. Available: https://www.upguard.com/blog/cve-2021-26855.

[7] S. Tzadik, "SIGRed – Resolving Your Way into Domain Admin: Exploiting a 17 Year-old Bug in Windows DNS Servers," Check Point Software Technologies LTD, 14 July 2020.

[Online]. Available: https://research.checkpoint.com/2020/resolving-your-way-into-domain-admin-exploiting-a-17-year-old-bug-in-windows-dns-servers/.

[8] "VE-2020-1350 Detail," National Institute of Standard and Technology , [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2020-1350#vulnCurrentDescriptionTitle.

[9] A. C. Heads-Up, "A vulnerability called “SIGRed” (CVE-2020-1350), exploits a buffer overflow within the way that Windows DNS Servers process SIG resource record types.," ASSURA, 28 July 2020. [Online]. Available: https://www.assurainc.com/a-vulnerability-called-sigred-cve-2020-1350-exploits-a-buffer-overflow-within-the-way-that-windows-dns-servers-process-sig-resource-record-types/amp-on/.

[10] b. Rudis, "Windows DNS Server Remote Code Execution Vulnerability (CVE-2020-1350): What You Need to Know," Rapid7, 14 July 2020. [Online]. Available: https://www.rapid7.com/blog/post/2020/07/14/windows-dns-server-remote-code-execution-vulnerability-cve-2020-1350-what-you-need-to-know/.

[11] maxpl0it, "CVE-2020-1350-DoS," maxpl0it, London, England, 17th of July 2020.

[12] D. D. S. A. R. HULSEBOS, "DANIEL DOS SANTOS AND ROB HULSEBOS," Forescout Technologies Inc, 27 July 2020. [Online]. Available: Major Vulnerability in Windows DNS Servers: Responding to CVE-2020-1350 (SIGRed).

[13] H. Aver, "CVE-2020-1350: Vulnerability in Windows DNS servers," Kaspersky Lab, 15 July 2020. [Online]. Available: https://www.kaspersky.com/blog/cve-2020-1350-dns-rce/36366/.

[14] "Windows DNS Server Remote Code Execution Vulnerability," Microsoft , 9 March 2021. [Online]. Available: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26897.

[15] M. Shah, "Threat Hunting for CVE-2020-1350: Microsoft DNS Server Vulnerability," Awake security, [Online]. Available: https://awakesecurity.com/blog/threat-hunting-for-cve-2020-1350-microsoft-dns-server-vulnerability/.

[16] "SIGRED/Wormable Windows DNS Server Remote Code Execution," Alert Logic, Inc, 15 July 2020. [Online]. Available: https://support.alertlogic.com/hc/en-us/articles/360045858812-07-15-2020-SIGRED-Wormable-Windows-DNS-Server-Remote-Code-Execution.

AUTHOR PROFILE

Jayasundara H. M. D. E. K. *Born in Negombo, Sri Lanka on 05th of October 1999. Studying at University of Sri Lanka Institute of Information Technology, Malabe, Sri Lanka. Received the certificate in INTRODUCTION TO CYBERSECURITY COURSE at Cisco Networking Academy, Sri Lanka, in 2020, INTRODUCTION TO IOT COURSE at Cisco Networking Academy in 2020 and NDG LINUX UNHATCHED COURSE at Cisco Networking Academy in year 2020. Following BSc (Hons) in Information Technology Specializing in Cyber Security degree, Sri Lanka Institute of Information Technology (SLIIT) University, Malabe, Sri Lanka, From February 2019 to February 2023. Mr. Jayasundara currently work as COMPUTER OPERATOR at R & R Foreign Employment Agency, Negombo. His primary research interests include Critical infrastructure security in healthcare sector, security vulnerabilities, and Cyber Crimes, Artificial intelligence, Internet of Things (IOT), and so on. He is a member of IEEE community at SLIIT, a Member of ISACA community in SLIIT and a member of Cyber Security Community in SLIIT. And he is currently studying in 3rd year 1st semester in his university life.*