**SLIIT**

Systems and Network Programming

Assignment 1

Madushanth R.K.U

IT19053042

**Introduction**

This study is to discover about the new kind of vulnerability Ghost Cat, which was found on earlier in this year (2020). Further this report discuss about the impact of that vulnerability, method and technique used to exploit.

**Ghost Cat CVE-2020-1938**

This is a high risk vulnerability which was created on 20th February 2020. It make huge impact on Apache Tomcat web server. Special care must be taken when using the Apache JServ Protocol alias AJP. AJP is a binary protocol designed to handle requests sent to web server destined for an application server in order to improve performance. Initially ghostcat was discovered by researchers at chaitin Tech and reported to the Apache software foundation.

* Impact of Ghost cat :

By exploiting the this vulnerability ,an attacker can read the contents of the configuration file an sources code files all webapps deployed on Tomcat. Attacker can inject a file containing malicious JSP script code to the server. This cause remote code execution at the end. It affect all version of Tomcat

Versions of tomcat are affected

* Apache Tomcat 9.x < 9.0.31
* Apache Tomcat 8.x < 8.5.51
* Apache Tomcat 7.x < 7.0.100
* Apache Tomcat 6.x
* Exploitation technique

AJP connector is enable by and the attacker can access the AJP connector service port and then there is chance of exploiting the vulnerability ghost cat.

* Exploitation method

nmap the local host, then by using the python code of CNVD-2020-10487\_scanner port can be opened then the request can be send. Finally by using the python code CNVD-2020-10487-master we can read the xml file

**Conclusion**

There are many Linux vulnerability found in this modern world. Likewise we use internet for various purpose so there is huge chance of getting attack. So as internet user we must study all kind of vulnerability to avoid those.

**Reference**

1. Tenable®. 2020. CVE-2020-1938: Ghostcat - Apache Tomcat AJP File Read/Inclusion Vulnerability (CNVD-2020-10487) - Blog | Tenable®. [ONLINE] Available at: <https://www.tenable.com/blog/cve-2020-1938-ghostcat-apache-tomcat-ajp-file-readinclusion-vulnerability-cnvd-2020-10487>. [Accessed 12 May 2020].
2. Akshay 'Ax' Sharma. 2020. Nexus Intelligence Insights: What's in a Ghostcat? CVE-2020-1938 Apache Tomcat - Local File Inclusion Potentially Leads to RCE. [ONLINE] Available at: <https://blog.sonatype.com/nexus-intelligence-insights-whats-in-a-ghostcat-cve-2020-1938-apache-tomcat>. [Accessed 12 May 2020].
3. CVE-2020-1938: Ghostcat vulnerability. 2020. CVE-2020-1938: Ghostcat vulnerability. [ONLINE] Available at: <https://www.chaitin.cn/en/ghostcat>. [Accessed 12 May 2020].