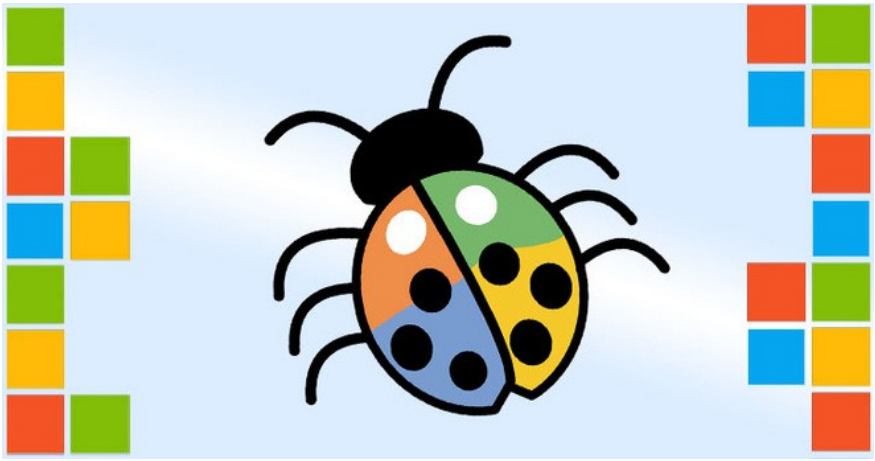
Top 5 most dangerous remote execution vulnerabilities in early 2020, some even automatically infect other computers without users knowing.

In the cybersecurity world, remote execution vulnerabilities are the most dangerous type when hackers can attack victims without physical access to the user's computer.

Remote Code Execution (RCE) is the most dangerous type of vulnerability, allowing hackers to take control of the application server, which can take important data from the organization or do it. springboard to strike deeper into the enterprise system.

Here are the top 5 dangerous RCE vulnerabilities newly discovered since the beginning of 2020, evaluated by the expert of Vietnam cybersecurity corporation based on the complexity, popularity and impact scale of these holes. this gap.



I. CVE 2019-2725: Remote code execution vulnerability on ORACLE WebLogic

Specifically, this security flaw is in the WLS9-ASYNC component on Oracle's Weblogic server that allows an attacker to import malicious XML data via specially designed paths without any permission, from it can gain access and execute arbitrary code on the Weblogic server.

This vulnerability is easily exploited by an attacker, since anyone with HTTP access to the WebLogic server can execute an attack. Moreover, it does not need user interaction, such as opening attachments or clicking on

malicious links, to download malicious code. Therefore, this error has a CVSS score of 9.8 / 10.

II. CVE 2020-0796: Remote code execution flaw on Windows SMB protocol

CVE 2020-0796 (RCE) is considered to be the most serious vulnerability when hackers can execute malicious code remotely without authentication on Windows 10, and can automatically infect other computers. .

SMB (Server Message Block) runs on port 445, is a network protocol that supports file sharing, web browsing, printing and network communication. This vulnerability is also known as SMBGhost, and stems from the way SMBv3 handles queries of the compression header, allowing remote attackers to execute malicious code on the server or client with privileges across the System.

III. CVE 2020-1938: Ghostcat vulnerability reads and inserts files on Apache Tomcat

CVE-2020-1938, also known as Ghostcat, is a flaw in Apache Tomcat's AJP (JavaServer Pages) protocol - a free and open source web server software, used to run programming web applications. in java language. This hole has a score of 9.8 / 10, the highest level.

According to VSEC Network Security Corporation experts, Ghostcat vulnerabilities have been discovered in all versions (9.x / 8.x / 7.x / 6.x) of Apache Tomcat released throughout. Over the past 13 years, and it is particularly serious that exploit codes have appeared and been shared widely on the internet, from which hackers can search and deploy hacking methods to the web server. easily.

IV. CVE-2020-7961 Unreliable data structure conversion vulnerability on Liferay

CVE-2020-7961 is a data structure conversion error on the Liferay platform - a widely used open source portal. This vulnerability allows attackers to take advantage of the data structure conversion functions that Liferay uses to insert malicious code, gain full control of the application and execute remote code to the server, perform actions. such as changing the look of websites, stealing data, .

This red hole exists on earlier versions of Liferay 7.2.1 CE GA2 and currently Liferay has released timely patches in versions Liferay Portal 7.1 GA4, 7.0 GA7 and 6.2 GA6.

V. CVE-2019-11469: SQL Injection vulnerability in ManageEngine Application Manager (MEAM)

The SQL Injection vulnerability exists in enterprise system management applications using ManageEngine Application Manager version 14072 and earlier, allowing an attacker to enter data into a website's database via parameters. send to server.

Hackers will take advantage of this vulnerability to gain control of the server by adding an administrator account with the highest permissions. Because ManageEngine requires logon access to the monitored servers, hackers can easily hijack the entire server infrastructure, extract critical data, and install malicious code across the system.

Currently, the vulnerabilities in these software and platforms have been patched by the developer, so if using them, VSEC recommends that businesses update to the latest version soon, as well as to disable the feature modules that are causing these vulnerabilities.

To help businesses understand the nature and dangers of each type of vulnerability, at the same time, they can check for themselves whether the system encounters the above-mentioned vulnerabilities and detail how to fix them if any. VSEC experts have also compiled a guide package, available free of charge at: https://vsec.com.vn/