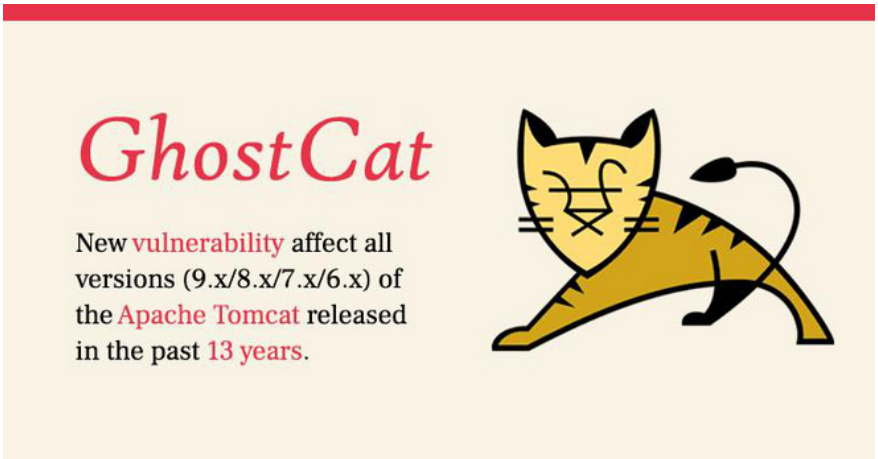
Detecting high-risk vulnerabilities potentially affecting 1 million servers worldwide

The vulnerability allows an attacker to read configuration files of the application, steal passwords or API tokens, and even hijack the server.

Ghostcat is a flaw in the AJP Tomcat (Apache JServ Protocol) AJP Tomcat protocol - a free, open source web server software used to run web applications programmed in the java language.

Although it is free software, Apache Tomcat is highly appreciated for its ability to set up a secure, cost-effective, and efficient website environment. That is why Apache TomCat is always on the list of the most popular open source software in the world today and is widely used by many units in the fields of finance, banking, and telecommunications. . Therefore, the appearance of vulnerabilities on this software is considered extremely dangerous.

The GhostCat vulnerability was tracked with code CVE-2020-1938 (CVSS 9.8), exploited by hackers in the form of special characters while sending requests to the server to read source code or configuration file information. server. Once these configuration files are acquired, hackers can gain access and install backdoors to gain remote control and execute other network attacks.



Severity.

According to VSEC experts, the Ghostcat flaw has now been detected on all versions (9.x / 8.x / 7.x / 6.x) of Apache Tomcat released over the past 13 years, and the It is especially serious that exploit codes have appeared and been shared widely on the internet, from which hackers can find and deploy methods of hacking into web

servers easily. T

In the BinaryEdge vulnerability search engine, there are currently more than one million Tomcat servers currently in operation, so VSEC experts emphasize that all businesses and individuals use apache tomcat without updating to the session. The latest version is all on the list of possible attackers' prey. Therefore, VSEC recommends that if businesses use the Apache Tomcat system, please update the system to the latest version, never open the AJP port to untrusted clients.

Tomcat team said: *'Users should note that a change has been made in the default AJP Connector configuration version 9.0.31. Therefore users who update to version 9.0.31 or higher will need to make minor changes to their configuration. '* However, if for some reason the user is unable to upgrade the affected server immediately, it can be fixed temporarily by turning off the AJP Connector, or redirecting it to a local port to avoid unnecessary risks to the server.