SaltStack has the most serious vulnerability ever, thousands of servers can be seriously affected

Unlike previous vulnerabilities, this one of SaltStack can affect all servers in the system, causing a much bigger impact.

SaltStack is a well-known open source software for configuration management and a tool to remotely control applications on the enterprise server, with the client-server model. Through SaltStack, a command server (master machine) can be easily remotely controlled and configured as a series of client servers (minions) below.

But recently, Vietnam Network Security Joint Stock Company has issued a warning about a security vulnerability called SaltStack RCE in this open source software. The vulnerability could have serious implications for the entire enterprise technology system by allowing hackers to remotely execute arbitrary code on servers in data centers or computing platforms. cloud.

The severity of SaltStack RCE is that it can be exploited to affect all servers in the system, instead of affecting only servers that have vulnerabilities. This shows that its impact level is many times larger than the previous holes.

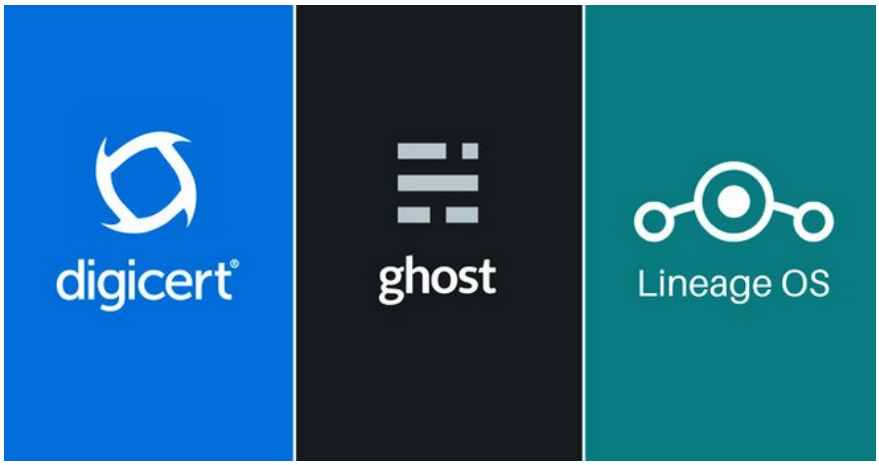
To successfully exploit this vulnerability, hackers will combine with 2 other SaltStack vulnerabilities (vulnerability CVE-2020-11651 and CVE-2020-11652, which existed in versions 3000.1 and earlier) to intervene. Interfering with data exchange process between master server and minion server.

Based on exploiting these two vulnerabilities, hackers can bypass authentication layers (based on CVE-2020-11651), and unauthorized control of directories (based on vulnerability CVE-2020-11652). , takes full control with not only the master server but also the entire minion server in the system. From there hackers can install malicious software, even spyware or malware to extort data into the enterprise system.

With the above level of danger and scale of influence, SaltStack RCE is extremely serious and is assessed by the Common Vulnerability Scoring System (CVSS) of the Department of Homeland Security's Infrastructure

Advisory Council. The US scored 9.8 / 10.

The flaw was discovered by researchers at F-Secure in early March and announced in early May 2020, shortly after SaltStack released and encouraged users to update to the new patch. A special patch for SaltStack Salt before 2019.2.4 has also been released.



Common server platforms may be threatened by this vulnerability.

According to Mr. Truong Duc Luong - General Director of Vietnam Internet Security Joint Stock Company, " *Currently, many large enterprises in the world are using SaltStack to support server management such as DigiCert Inc., LineageOS . In Vietnam, many enterprises providing IT infrastructure and services are also using this open software.If the infrastructure of these businesses is attacked, it can lead to servers, data of customers. leaked goods, affecting hundreds of thousands of businesses* ".

VSEC experts recommend users to install automatic update mode for SaltStack to ensure the system always uses the latest security patches. Tighten access to the master server, narrow the range of devices that can access the SaltStack 4505 and 4506 default ports.