Thousands of servers are affected by the flaw on SaltStack RCE

Vietnam Cyber ??Security Joint Stock Company (VSEC) has just warned of the SaltStack RCE security error - a serious flaw discovered on SaltStack that could seriously affect the entire information technology system of the enterprise. .

Accordingly, this vulnerability allows hackers to execute arbitrary code remotely on servers located in data centers or on cloud platforms.
The flaw was discovered by researchers at F-Secure in early March and announced in early May, shortly after SaltStack released and encouraged users to update to the new patch. A special patch for SaltStack Salt before 2019.2.4 was also released.
SaltStack is an open source software, used for configuration management and a tool to remotely control applications on the enterprise server, operating with the client-server model. Where a command server is called a master, and the server that receives commands from the master server with different operating systems is called a minion.
In order to successfully exploit this vulnerability, hackers used a combination of two error codes, namely CVE-2020-11651 and CVE-2020-11652, that exist in versions 3000.1 and earlier of SaltStack to interfere with data exchange between the master server and the minion servers in it. CVE-2020-11651 is a vulnerability to bypass authentication and collect tokens of users while CVE-2020-11652 is a vulnerability that allows unauthorized access or control of directories through failure to control input variables. .
If other vulnerabilities after being exploited only impact on the server that exists, the vulnerability of SaltStack RCE can affect the whole server in the system with a much greater impact level. Hacked hackers can bypass authentication and collect control keys of minion machines with the highest user rights, and can gain unauthorized control of directories, gaining full control over not only the master server but also with all minion machines. From there, an attacker can illegally install malicious programs, bitcoin mining software, even install on spyware or cryptographic malware to extort data.
Given the aforementioned degree of danger and scale, SaltStack RCE was rated extremely serious and was scored 9.8 / 10 by the Advisory Board's Common Vulnerability Scoring System (CVSS). The infrastructure is part of the Department of Homeland Security.
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.