

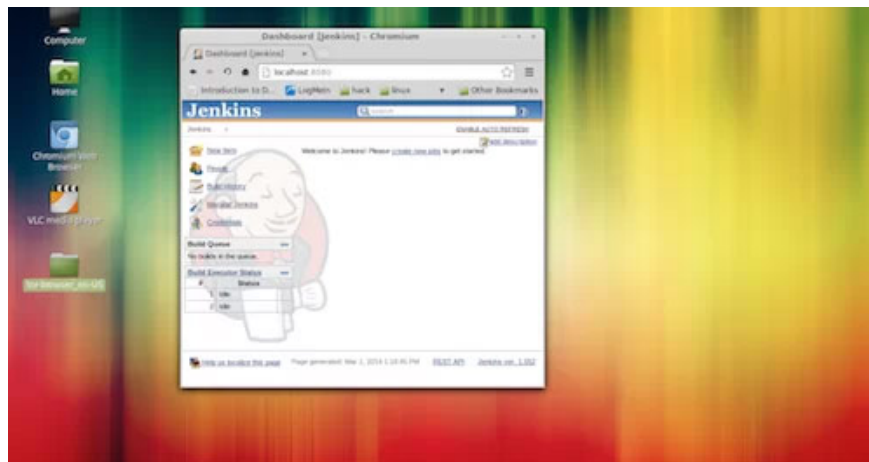
Warning: Jenkins exists a serious security hole that helps hackers gain control of computers of many Vietnamese businesses

Last night, September 18, VSEC - Vietnam Cyber Security Joint Stock Company issued an emergency warning about a serious security hole in the open source application Jenkins.

Last night, September 18, VSEC - Vietnam Cyber Security Joint Stock Company issued an emergency warning about a serious security hole in the open source application Jenkins. If successful exploitation of this vulnerability, hackers can execute unauthorized commands remotely. This serious flaw could affect the computer systems of many Vietnamese businesses.

1. Sim vulnerabilities threaten more than 1 billion phones globally
2. Warning: 600,000 child navigational devices may be hacked, parents should be careful

According to VSEC, this vulnerability, coded as CVE-2019-10392, was assessed as dangerous as October 8, discovered by Dutch security expert Francesco Soncina. Taking advantage of this vulnerability, hackers can easily gain control of the server, control the entire information system of the enterprise, thereby conducting illegal activities such as spreading confidential data, stealing information. believe...



VSEC security experts said that to successfully exploit this vulnerability, hackers need to have a user account with the right to configure 'Git Client Plugin' and 'Job / Configure (USE_ITEM)' from version 2.8.4 and above. ago. An important factor that allows hackers to execute unauthorized code on the server is the failure to control the input value at the Repository URL parameter in the Git Client Plugin.

Currently, CI (Continuous Integration) system is quite popular among high-tech enterprises in Vietnam. 80% of them have CI system using Jenkins application.



VSEC experts said that on the Internet, there are currently more than 200,000 servers installing Jenkins with the flawed version.

VSEC recommends organizations and businesses to do the following to avoid being affected by this serious flaw.

1. Quickly update Jenkins' Git Client Plugin for the latest version.
2. Publicly restrict systems in use on the intranet.
3. Configure Whitelist of IPs to access critical systems.
4. Set strong passwords for system accounts, including low-power accounts.

You finished reading the article "**Warning: Jenkins exists a serious security hole that helps hackers gain control of computers of many Vietnamese businesses**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.