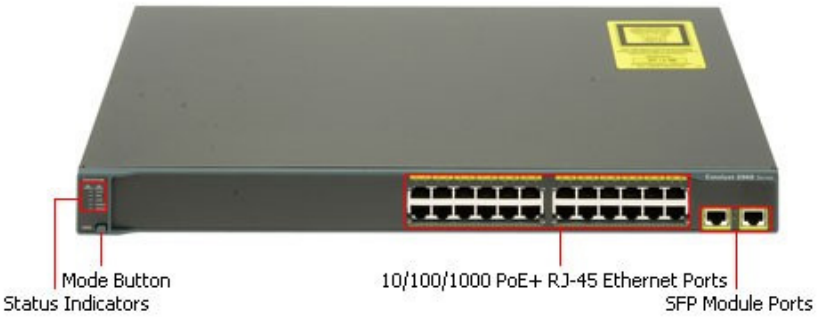
Warning: Detecting more than 1000 Cisco router and switch devices in Vietnam has a serious security error

There are more than 1000 Cisco router and switch devices in Vietnam (all devices used in large network environments and core systems) are subject to serious security errors.

There are more than 1000 Cisco router and switch devices in Vietnam (all devices used in large network environments and core systems) are subject to serious security errors.

The Information Security Department (Ministry of Information and Communications) has sent a warning letter about a group of 40 critical safety information points on Cisco routers (switches) and switches (switches). In particular, in the vulnerable Cisco IOS operating system with international error code CVE-2018-0171 exists in the Smart Install function, a function used to manage installation, device deployment and is normally enabled determined.



Bad guys take advantage of this flaw to send a Smart Install fake message to the TCP port 4786 of the device. If successful, a process will be started to reload the device, execute remote code or perform an infinite loop on the device that leads to a denial of service.

Previously, Cisco confirmed information about this vulnerability on its router / switch devices on March 28, 2018. Since then, the CVE-2018-0171 vulnerability has been exploited by bad guys to carry out many cyber-attacks around the world.

According to VARANS, there are more than 1000 devices affected in Vietnam and the country with the most IP range detected. Therefore, users need to be very wary.

The list of Cisco network devices is affected by the vulnerability:

STT	Thiết bị
1	Catalyst 4500 Supervisor Engines
2	Catalyst 3850 Series
3	Catalyst 3750 Series
4	Catalyst 3650 Series
5	Catalyst 3560 Series
6	Catalyst 2960 Series
7	Catalyst 2975 Series
8	IE 2000
9	IE 3000
10	IE 3010
11	IE 4000
12	IE 4010
13	IE 5000
14	SM-ES2 SKUs
15	SM-ES3 SKUs
16	NME-16ES-1G-P
17	SM-X-ES3 SKUs

In order to ensure information security and prevent the risk of network attacks, administrators at agencies and organizations check and review network devices that may be affected and fix vulnerabilities.

How to check CVE-2018-0171 vulnerability

To check CVE-2018-0171 vulnerability, administrators can do one of the following:

Method 1: Use tools published by Cisco at the following link: https://github.com/Cisco-Talos/smi_check

Method 2: Run the **show vstack config** command on the Cisco device. If the device uses the Smart Intstall Client, the following content will appear:

switch # show vstack config | inc Role

Role: Client (SmartInstall enabled)

How to fix security holes on Cisco routers and switches

Method 1: Update and upgrade the operating system for routers and switches according to Cisco's instructions at the following address:

1. https://goo.gl/tbYqPu

Method 2: Run the no vstack command on the affected device to turn off the Smart Instal feature if not needed.

Method 3: If you don't use Access List, you can block 4786.

For more information on vulnerability analysis and PoC, you can visit the link below.

1. https://goo.gl/hc8saV

See more:

1. Warning: GandCrab extortionist code is attacking Vietnam
2. Warning of new malware appear like Wannacry, capable of deleting Vietnamese percussion on computer
3. Appearing dangerous Android malicious code specializing in stealing chat content on Facebook Messenger, Skype .