Hundreds of thousands of IoT devices are likely to be attacked by vulnerabilities on the server

On Christmas Day, a vulnerability affecting web servers was embedded with hundreds of thousands of IoT devices, namely GoAhead, a web server created by Embedthis Software.

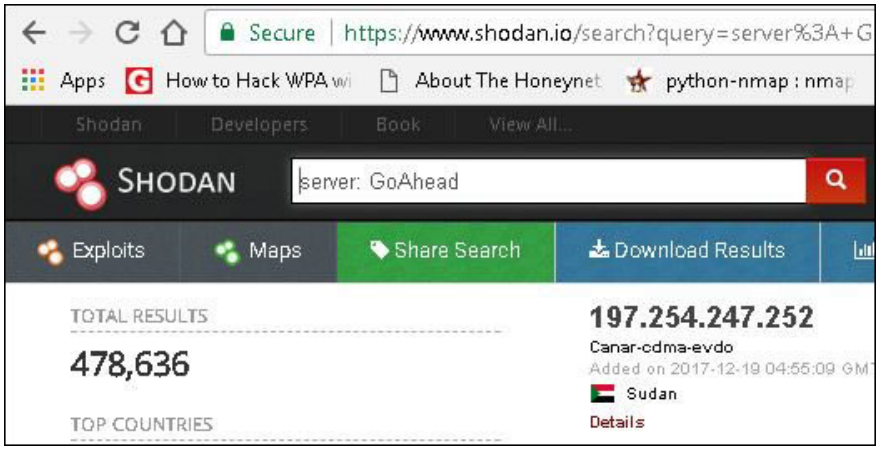
On Christmas Day, a vulnerability affecting web servers was embedded with hundreds of thousands of IoT devices, namely GoAhead, a web server created by Embedthis Software.

On its home page, Embedthis said that their products are currently being developed inside products of many big names like Comcast, Oracle, D-Link, ZTE, HP, Siemens, Canon .

This web server is quite popular with hardware manufacturers because it can run on a variety of devices, including IoT devices, routers, printers .

The GoAhead server is executing remote code

Researchers from Elttam have discovered how to execute remote code on GoAhead web server devices, vulnerabilities code number CVE-2017-17562. An attacker could exploit this vulnerability when CGI is enabled. This is a dynamic link program that allows communication between server and program quite popular.



Hundreds of thousands of IoT devices are capable of being attacked

About 500 thousand to 700 thousand devices affected

Elttam reported a bug to Embedthis and the company quickly released a patch. All versions of GoAhead before 3.6.5 are capable of being attacked, but errors are only validated on version 2.5.0.

Embedthis has done its work, but now everyone who has a GoAhead server must update it quickly. According to Shodan estimates, there are 500,000 to 700,000 devices on this list.

See more:

1. Billions of devices are affected by the new Bluetooth attack
2. Internet of Things - IoT or What is the universal connection network?
3. Internet of Things - opportunities and challenges for businesses