Security vulnerabilities threaten more than 1 billion Android smartphones

The vulnerability allows malicious apps to deploy and disguise any pre-installed software on the machine and display a fake interface to trick users into using it.

Norwegian security experts have discovered a serious security vulnerability called Strandhogg (CVE-2020-0096) that affects the Android operating system, allowing hackers to deploy various types of attacks with fake forms. different appearance. First discovered in late 2019, Strandhogg has been successfully deployed by a number of attackers on a victim's machine to steal banking information and multiple login accounts, and track activity on the device.

With the new name of Standhogg 2.0, this new security flaw affects most devices running Android, except for devices running the latest version of Android 10 (Android Q). However, the platform is only available on about 15-20% of all devices using Google's mobile operating system worldwide, which means there are over 1 billion devices capable of being exploited.

Strandhogg 1.0 exists in Android's multi-tasking feature, while version 2.0 is essentially a privilege flaw that allows hackers to gain access to most applications available on the device.

When the user touches the icon of any legitimate application on the device, the malware will exploit the Strandhogg vulnerability to block and hack this operation to show a fake interface to the user instead of opening the application. real use.

Strandhogg 1.0 can only attack one application at a time, while 2.0 allows hackers to actively attack almost every software available on the device with a single touch and requires no preconfiguration for each. target program.

According to *THN* , Strandhogg 2.0 contains many dangers and worries because the victim is almost unable to detect the attack. This vulnerability is able to hack and tamper with the interface of almost any application present on the device without configuration, used to require all permissions on the device. Besides, version 2.0 can be used on all Android devices (except for Android 10) without requiring root access and does not require any permission to operate.

In addition to stealing account information, malware can increase the level of danger by deceiving users to grant sensitive access on the device when posing as a legitimate application.

'Hackers can take advantage of Strandhogg 2.0 to gain access to messages, private photos, steal account logins, track GPS activity, make or record calls or track through Camera and microphone of the phone. Meanwhile, anti-virus programs or security scanners are difficult to detect malicious applications to give warnings to users', the research team said.