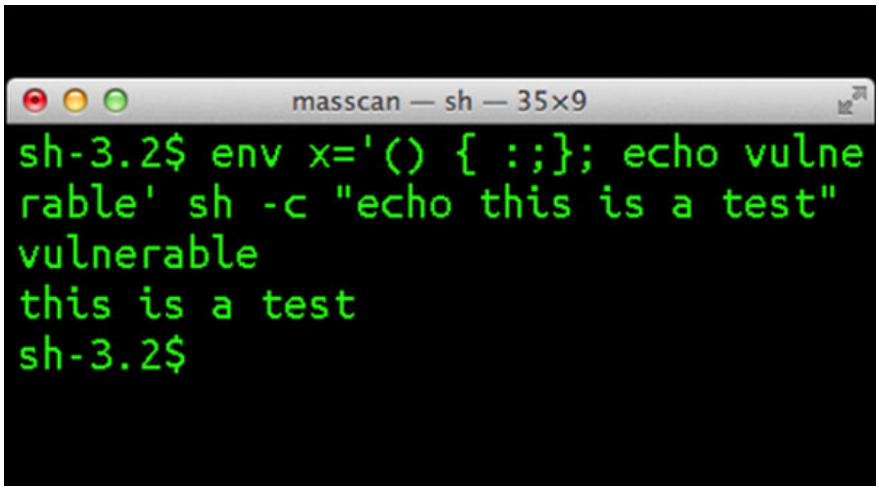
Safeguard against Shellshock security vulnerabilities

The main advice for computer users is to always check for the latest software updates as soon as possible.

The main advice for computer users is to always check for the latest software updates as soon as possible.

As mentioned recently, Shellshock is the name of a recently discovered security vulnerability that can directly affect the Bash application (Bourne again shell) - allowing bad guys to attack and control remote unprotected Linux or Mac systems.



To determine if the system is compromised by Shellshock security vulnerabilities, first open the Terminal interface, execute the following command:

env x = '() {:;}; echo vulnerable 'bash -c "echo this is a test"

width = "600"

If your Mac OS X or Linux computer system is potentially at risk from the security hole, the Terminal interface will return the results shown below (you will see the **'Vulnerable' message** line appear immediately). above the line 'this is a test')

Conversely, if the system has been patched and protected, the Terminal interface will show the message line:

$ env x = '() {:;}; echo vulnerable 'bash -c "echo this is a test" bash:

c?nh báo: x: ?ang b? qua function xác ??nh th? bash: l?i

nh?p s? xác ??nh function cho 'x' này là m?t th?

width = "600"

So if you get the **'Vulnerable'** result, what do you have to do with the system that is at risk? First of all you need to be calm even if you are just a normal computer user. If the computer you are using is behind the protection of a firewall, the possibility of being attacked from the security hole Shellshock has also been significantly reduced - because the bad guys have no way to execute malicious code. harm through the Bash shell on your computer system, unless the bad guys can somehow fool you into executing them right on your computer.

If you are a MAC OS X user, you can rest assured that Apple has also confirmed that with OS X, the system is guaranteed to be safe by default and bad guys will not be able to attack remotely via Bash. shell, unless the user configures using advanced UNIX services. Apple also said it is aggressively deploying a software update for its advanced UNIX service users.

As for Linux, users should not be too frightened because most of the names' distributions such as Red Hat, Ubuntu, Debian, Fedora, CentOS already have these Shellshock security patches. However, according to Red Hat, the code name code CVE-2014-6271 is still incomplete and is still being updated with new updates to enhance user protection. Therefore, as a Linux user, always pay attention to be ready to install the latest updates for your system.

As previously mentioned, Shellshock not only affects computer users but also network devices and Internet-capable devices (IoT). Therefore, the best way to ensure the safety of the patched computer system is the latest firmware update for the network devices you are using.

Besides, in addition to updating the latest patches, firmware, users should also avoid opening suspicious links and emails. You should also not trust the addresses displayed by dragging on each strange link - because hackers now have enough ways to use a valid link to fool you.

Finally, to protect yourself, make sure that anti-virus software, firewalls and devices designed to protect you always get the latest updates.