

# Security Advisory on “Shellshock” Bash Vulnerability

Publish Date: October 11, 2014

**This advisory applies to all Yealink products running all firmware versions.**

## Summary

Shellshock is a bug in a piece of software known as “Bash” that runs the command prompt on many Unix computers, including some Linux servers that run websites, and tiny computers inside consumer devices such as routers, web cams and phones.

## Risks

Through the vulnerability in Bash versions from 1.13 to 4.3 (almost involves all its public release versions), the malicious software can take control of an infected machine, launch denial-of-service attacks on websites to disrupt their operations and scan for other vulnerable devices, including routers.

This exploit is consistent with CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-6271, etc. For more information, refer to

<http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2014-6271>

## Security Advisory

We have carefully inspected our products in all versions, and here we announce that Yealink products are not affected by the Shellshock Bash vulnerability. Yealink will follow up this security issue and update the security advisory to users for any changes in the future.

Product Name	Version	Vulnerable
SIP-T19/SIP-T19P	All Versions	Not Vulnerable
SIP-T20/SIP-T20P	All Versions	Not Vulnerable
SIP-T21/SIP-T21P	All Versions	Not Vulnerable
SIP-T22/SIP-T22P	All Versions	Not Vulnerable
SIP-T26P	All Versions	Not Vulnerable
SIP-T28P	All Versions	Not Vulnerable
SIP-T32G	All Versions	Not Vulnerable
SIP-T38G	All Versions	Not Vulnerable
SIP-T41P	All Versions	Not Vulnerable
SIP-T42G	All Versions	Not Vulnerable
SIP-T46G	All Versions	Not Vulnerable
SIP-T48G	All Versions	Not Vulnerable
VP530	All Versions	Not Vulnerable

Product Name	Version	Vulnerable
W52P	All Versions	Not Vulnerable
Redirection and Provisioning Service	All Versions	Not Vulnerable