Security Advisory on “Heartbleed” OpenSSL Vulnerability

Publish Date: 2014-4-18

This advisory applies to all Yealink products using OpenSSL from version 1.0.1 to 1.01f.

Summary

Heartbleed is a security bug in the open-source OpenSSL cryptography library, widely used to implement the Internet's Transport Layer Security (TLS) protocol. This vulnerability results from a missing bounds check in the handling of the Transport Layer Security (TLS) heartbeat extension, the heartbeat being why the vulnerability got its name.

Risks

Through the vulnerability in OpenSSL versions from 1.0.1 to 1.0.1f, an attacker can capture memory from the host 64k at a time. In this way, the attacker succeeds to capture the desired data, like the server’s private key, or the user’s password.

This exploit is consistent with CVE: 2014-0160.

Security Advisory

We have carefully inspected our products in all versions, and here we announce that Yealink products are not affected by the Heartbleed OpenSSL 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-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
W52P	All Versions	Not Vulnerable
Redirection and Provisioning Service	All Versions	Not Vulnerable