Reports of Security Vulnerabilities

We have received reports stating that there are security vulnerabilities in the Yealink range of phones. Yealink (UK) Limited has investigated these reports and has determined that the security vulnerabilities were the result of users not changing the default passwords.

Yealink produces a high quality product with sophisticated and advanced functionality. In any product of this nature there is the possibility of unauthorised use if reasonable steps to protect the device are not taken. This issue is not restricted or unique to Yealink product, but to any device where the password integrity is not maintained by the user. Users are especially vulnerable when using a phone on a public IP address.

RECOMMENDATIONS

As with all IT equipment it is important that users maintain good working practice in relation to password integrity. In order for security to be maintained over our product, the passwords at user and admin levels must be changed from the defaults.

Yealink take our customers' security very seriously and are constantly working to enhance the security features of the product even further. It is also therefore our recommendation that customers regularly update firmware to the latest version to benefit from our new features and facilities. The latest firmware can be downloaded from http://www.yealink.co.uk/downloads/

T18P	18.0.23.2
T20P	9.60.23.16
T22P	7.60.23.16
T26P	6.60.23.16
T28P	2.60.23.16
T38G	3.0.23.3

In conclusion to safeguard your Yealink phone we recommend that users change both the user and admin passwords and update to the latest firmware.