Statement

Yealink is a well reputed audio and video equipment manufacturer that has always attached great importance to product safety and compliance. Since its establishment, Yealink has been working hard to provide customers with better products and services. We are proud to have the majority of European operators amongst our customers.

Recently, we were contacted by a person who shared his concerns about the IP phones and compliance of Yealink. This person has communicated with us many times, and we thank him for his feedback to which we have responded. We have also learned that journalists have sent questionnaires to Yealink's customers or potential customers. Yealink would like to share the following information.

1. Product Safety

(1) Telephone devices only

Yealink wants to emphasize that the issues that were brought to our attention by the person concerned only regarded the telephone devices and did not relate to any other products.

(2) Yealink is devoted to product safety

Potentially Yealink phone firmware file can be unpacked in older phones according to our informant. After receiving this feedback, Yealink has checked the phone firmware and found that the problem is only for the old version of Yealink phones which have been end of sale from the market for years. Even if the file can be unpacked, it does not lead to personal configuration information leakage[1]. Considering that some customers may have concerns about the issue, Yealink has updated the firmware of the affected models. Customers who need it can contact the distributor or Yealink technical support to obtain the latest version.

The person concerned states that there is a security problem with the RSA tool, and the default

[1] According to our checks, there are a small number of customized versions that have built-in AutoProvision URL/user name/password that may be leaked, but even if a user obtains the built-in information, they cannot directly obtain the phone configuration file from the Auto Provision server. Because there are other security measures in auto provision s ever, such as IP whitelist, MAC /UA authentication, which can effectively prevent unauthorized/untrusted devices from auto provision server to download to the configuration and personal information.

key information when using the RSA tool is directly disclosed in the tool. It is important to note that the default key information is only a demo, and customers will normally use their own key to achieve batch deployment when needed. Due to the fact that few customers may use the default key for official purposes, we have turned off the default key on the latest RSA tool and reminded customers to set their own key in the usage guide.

He further suggested to Yealink that there is a security problem in the opening port of 5060, but according to the current communication, his understanding may be biased. In fact, Request for Comments (that is RFC) stipulates the specification of using port 5060. 5060 is one of the commonly used ports of the SIP protocol. We open the port complying with the RFC protocol. In addition, if the port receives a non-SIP message packet, it will actively discard it, which will not cause security risks.

The person concerned also mentioned YMCS to us. YMCS is Yealink's terminal device management cloud platform deployed on Amazon Web Services and Microsoft Azure. In order to ensure the security and compliance of this platform, Yealink entrusts Deloitte to conduct SOC2 Type2 audits for security and confidentiality every year. Yealink has always complied with GDPR rules, and the platform has also been certified by TÜV Rheinland on GDPR.

In fact, Yealink attaches great importance to security. Except for SOC2 Type2 audit and GDPR certification, Yealink's products have passed the security penetration test of third-party authoritative laboratories in Europe and America; Yealink has passed ISO27001 certification, the world's most widely recognized management system in the field of information security and Yealink has formulated applicable security white papers for different products. These actions and their results strongly prove Yealink's efforts and achievements in security work, as well as our ability to provide customers with safe and stable products and services. With the development of technology, Yealink will continue to invest resources and energy to ensure the safety and stability of products at the greatest extent. (If you want to know more about Yealink security and compliance, please check https://www.yealink.com/en/onepage/trust-center-overview).

(3) Yealink abides by GPL open-source obligations

Yealink has been committed to the development of enterprise compliance, and also abides by the open-source obligations of the GPL. Yealink initially disclosed the usage information of open source at https://www.yealink.com/en/onepage/open-source-software-yealink-phones. Later, we improved support.yealink.com, and migrated the open-source information to support.yealink.com-

>Help Desk, further optimized the content of open source and made it more convenient for users to obtain all technical materials at support.yealink.com. In order to avoid duplication, we deleted the original open-source link. At the same time, Yealink also provides the special consultation channel for this purpose. If customer has any questions about open-source software, they can send an email to security@yealink.com, and we will reply and answer in time. In addition, by scanning the QR code in the product QSG (Quick Start Guide), you can also know the usage of open source, and we also placed the official website link in QSG for users to query at any time. (https://www.yealink.com/website-service/download/offer-source-of-open-source-software.pdf)

In addition, the person concerned pointed out to Yealink that open-source modules, such as PJSIP and so on, have security issues caused by old versions. In practice, we will continue to make timely patches to solve the security vulnerabilities disclosed by open-source modules and entrust third-party laboratories to conduct security penetration tests to ensure the security of the phone system.

2. Yealink Company Compliant operation

The person concerned shared with us that Yealink (Europe) Network Technology BV's (hereinafter referred to as "**Yealink Europe**") operation is not in compliance with formal corporate requirements. Yealink is an open and transparent Chinese listed company, neither the shareholders nor the management team have any government background. Since its establishment, Yealink has always paid great attention to compliance and standardized operations. Yealink Europe is a wholly owned subsidiary of Yealink, established in the Netherlands to meet the requirements for Yealink's operations in the EU.

Finally, we would like to emphasize again that Yealink has always attached great importance to product safety and compliance since its establishment and devote to provide customers with the best products and services. We are always willing to communicate with professionals and discuss issues of product safety and business compliance. It will not only help Yealink improve better products and services for customers, but also help promote the progress of the industry. We will continue to develop products and services, pay attention to business compliance, commit ourselves to serve the market with better products, and contribute to the development of the industry.

Yealink Network Technology Co., Ltd.

July 13, 2023