Lydis statement on Follow The Money - press

On 16 September 2023, two articles were published on the journalism platform Follow The Money and in business newspaper De Tijd, stating that several organizations were using communication equipment from Chinese company Yealink in which security vulnerabilities had been discovered.

These articles had not been previously verified with Lydis or Yealink and contain demonstrable factual inaccuracies that give a false impression about Yealink, its equipment, and networked audio and video communications in general.

Lydis and Yealink were notified of issues with Yealink telephony equipment in August 2022. Yealink's video equipment (such as Teams) is completely excluded from these issues. This is completely secured by Microsoft and is only usable if these devices meet certain requirements. As a distributor, we naturally also strive to maximize the security of our products, and Lydis is very grateful to the person who reported these issues. Lydis was not aware of this situation, but after consulting Yealink, we discovered that there were indeed problems.

Much of the article deals with the issue of the encryption tool which, according to professional telephony providers, is not used to encrypt configuration files (the provisioning documents mentioned in the article). These providers use their own security measures, together with the security measures in the product, to ensure that data is exchanged securely between their platform and the equipment at the user's desk.

A person's phone subscription details are never obtained by the product manufacturer. This data is owned by the provider from which someone purchases a telephony service and the product communicates directly with the provider's server, without Yealink's intervention.

The port mentioned, 5060, is essential for the operation of phones and is used as the default port for VoIP communication. To make it clear, if this port is closed, a phone cannot function. The use of this port is not unique to Yealink products, but is used by all manufacturers in the VoIP industry.

The problems with the encryption tool and the issue of unlocking firmware could occur with some customers, in principle. Therefore, Yealink has updated the firmware of the severely outdated models, despite the fact that the firmware has not been supported for years. A modification has also been made to the encryption tool. We openly communicated this to affected customers in April 2023. Some of them then concluded, after analyzing and doing pen tests, that this did not create any additional risk for them. We would therefore like to stress that no personal data was at risk as a result of this situation.

Follow The Money and De Tijd touch on some outdated issues and products, falsely painting the picture that communication traffic from Dutch and Belgian institutions is at risk. That is absolutely not the case.

In June 2023, the person who reported the problem and a journalist from Follow The Money visited our office, and we explained everything in detail to them. It is therefore unfortunate to see that they did not include our explanations and information in the article.

Lydis has worked with Yealink for decades and, like the partners who carried out the pen tests, we see no reason to question Yealink's handling of security. Yealink takes systems security very seriously and, in our opinion, responded appropriately as soon as these issues came to light. If you have any questions, you can of course contact us.

On behalf of the Lydis team,

Gijsbert Zijlstra
Technical Director
gijsbert.zijlstra@lydis.com

Yealink's full statement can be found here, Yealink shares factual information here on all measures regarding security of its products and organization, such as ISO 27001, GDPR, SOC2 Type1, SOC2 Type2, and SOC3, 802.1x, AES Encryption.