Technical content clarification letter

To address our partners' concerns, Yealink wishes to provide a detailed technical response to the core questions in the article.

Topic	Details in report	Yealink comments
Device Management Platform	1. The YDMP collects and retains the WAN IP of the U.S. device and it also its private network IP creating useful attack data that is stored on a server controlled by persons within the jurisdiction of the PRC. 2. A Yealink employee in China, acting as a YDMP administrative user, can initiate a packet capture for traffic on the Ethernet and WAN switches in the phone. This means corporate users' information and behavior can be surveilled. 3. The T54W delivers users call detail records to the YDMP when it is registered with that platform. 4. A Yealink employee in China, acting as a YDMP administrative user, can initiate a call recording from the portal, store the recording in the T54W and then upload it to the YDMP. 5. The YDMP service agreement requires users to accept the laws of the PRC and arbitration of disputes in Xiamen province. In addition, the agreement's privacy policy does not include any references to international data protections such as GDPR.	The YDMP device management platform is an optional value-added service provided by Yealink, which was developed by Yealink to meet the needs of customers for the purpose of device deployment and trouble shooting. YDMP is locally hosted by the customer and Yealink does not have any access to these deployments. The platform has obtained the compliance assessment certification of Rheinland GDPR (General Data Protection Regulation). The platform data is primarily stored in well-known cloud service providers in the United States and Europe, user data and privacy security are 100% guaranteed.(Rheinland GDPR compliance assessment certificate query: https://www.certipedia.com/certificates/50479079?locale=en)
Device Management Platform	The Yealink Device Management Cloud Service Agreement is embedded as a PDF in Appendix C and is also available at this link: https://www.yealink.com/news_171.html Specific items of concern include: II.A: No real privacy and protection of PII (e.g., no references to GDPR) III.B.1: No reciprocal indemnification (one-sided) IV.B.2. 3. 6: No real privacy and protection of registration information IV.C: They can monitor use of the service IV.D: Public disclosure of use of service VIII.A: PRC governing law VIII.B: Mediation in Xiamen	It's 18-year official website privacy policy, privacy policies have also been updated. The privacy policy of the platform has always been updated with local policies and regulations. Users can see it when logging in to the platform and need to explicitly confirm their consent before they can accept the service. At the same time, users can exercise their rights of data control and management by operating or contacting us according to the methods described in the privacy policy on the platform, and there is no situation where they cannot control their personal data. In addition, in terms of data security protection, we fully apply all local regulations for product sales. For example, if the data is related to EU citizens, we comply with the relevant regulations of GDPR.
Device Management Platform	A Yealink employee in China, acting as a YDMP administrative user, can initiate a call recording from	In order to meet the user's quality of call management (QOE), we provide a recording function in YDMP (this function is disabled by default), but only when the user actively

	the portal, store the recording in the T54W and then upload it to the YDMP.	participates, that is, the user actively inserts a USB flash drive into the phone and enables the recording function. YDMP cannot record without the active participation of the phone user. This function is not available on any Microsoft Teams devices.
T54W Behavior Under Default Settings	During normal operations the Yealink phone communicates with a server located in Chinese controlled AliCloud infrastructure, without the permission of the owner/user or notice that it performs this activity of the phone.	The so-called 'Chinese Server' mentioned here refers to the Yealink RPS server, which is a server deployed in the United States, and only serves as a redirection deployment server for Yealink SIP Phone, which is an option provided by mainstream SIP Phone manufacturers. Value-added services. If Yealink's operator partner uses the RPS service, Yealink SIP Phone will actively initiate a request to the RPS server during the startup process of the first deployment, thereby redirecting to the operator's deployment server. If the RPS service is not used, Yealink SIP Phone will request three times, and then terminate the connection with the server. Moreover, during the request process, the factory information of the device is transmitted, and no customer data transmission and sharing will be performed. In addition, the RPS request initiated by the SIP Phone will use HTTPS to ensure the security of interaction.
T54W Behavior Under Default Settings	Yealink's IP phone has the potential to be used to conduct network surveillance of the customer's IP network because the phone's default configuration does not require voice and data transmission on separate Virtual Local Area Networks (VLANs), unless the customer has already set up its router to manage separate VLANs for its IP phones. However, separate VLANs can be custom configured by the VoIP service provider as part of its installation processes—in a variety of ways.	Regardless of whether the phone is assigned a separate VLAN, the IP phone does not have the ability to monitor the network, and all network information is managed by the switch of the enterprise intranet. The protocol for obtaining VLANs is LLDP/CDP, which is a standard formulated by 802.1ab and Cisco in the communication industry. Only the routers and switches of the customer's enterprise IT administrator can record and view these VLANS information.
T54W Behavior Under Default Settings	Default login credentials make the Yealink phone susceptible to attack. The Yealink phone uses common login credentials, known by most security/pen testing assessment tools: admin/admin. The phone does not force the administrator to create a new login or password when the phone is initially configured, though it does show a fairly low-key reminder to do so, as can be seen in various configuration screenshots in Appendix E.	During the actual deployment of the phone, the operator/service provider will change the default password.

T54W Behavior Under Default Settings	The Yealink phone is made vulnerable because it comes pre-configured to accept credentials for connection and access to the device from 187 “trusted” digital certificate authorities (CAs). The specific vulnerability is that use of any of these certificates provides trusted access to the administrative interface of the T54W. It requires knowledgeable action on the part of the user company’s administrator to edit the list of trusted certificate providers to remove any that are risky. The T54W is highly susceptible to unauthorized remote access, from which a device or general network attack can be initiated. The T54W comes preconfigured to accept digital certificates from 187 certificate authorities for remote access. One of the certificate authorities, based in China, has been blocked by Google for irresponsibly facilitating Man-In-The-Middle (MITM) attacks on web traffic.	A CA certificate is an authoritative electronic document used to prove the legitimacy of the identity of a subject (such as an organization), also known as the network's ID card. Most devices and operating systems have CA certificates installed by default. The built-in CA certificate of Yealink is mainly used for two-way security verification with the platform that users need to connect to. T54W runs Linux OS system, and T54W actually has only 97 certificates, not the 187 mentioned in the article, nor the 2 CA certificates mentioned in the article (China Internet Network Information Center EV Certificates Root/ CNNIC ROOT). The two CA certificates mentioned in the article are actually the certificates pre-installed in the Android system by Google, not in T54W.
T54W Behavior Under Default Settings	The Yealink phone provides no option of protecting the administrator login with multifactor authentication nor any protection from brute force credential stuffing attacks by locking the account after a number of unsuccessful attempts.	The phone is deployed inside the enterprise and managed by IT uniformly. The administrator will modify the password, and the security level of the password is sufficient to ensure the security of the device; at the same time, if the user enters the wrong password three times, the web page of the phone will be locked, and there is no unlimited brute force cracking.
T54W Behavior Under Default Settings	Port/Protocol Discovery (port scan) showed the following: PORT STATE SERVICE 53/tcp open domain 80/tcp open http 443/tcp open https 5060/tcp open sip 5061/tcp open sip-tls MAC Address: 80:5E:C0:84:C0:80 (Yealink(xiamen) Network Technology) We recommend that manufacturers, by default, close ports 53, 80 and 5060 to ensure only secure communications are occurring. If the customer wishes to open them up then that is a custom configuration for them.	The test uses 2-year-old firmware. In fact, the latest version has enabled HTTPS by default, and the default port opened by the phone is the established communication port in the industry.
T54W Behavior Under Default Settings	When the phone was acting as an Ethernet switch for an attached device, we did not observe any pattern of traffic rerouting, either voice or data.	The PC port of the phone is only used as a switch port, and the phone cannot capture the data of any connected device from the PC port.

T54W Behavior Under Default Settings	In addition to the Linux kernel, we observed two other open-source modules by extracting strings from the root volume: LightHTTPD HostAPD We cannot conclude with any certainty that the open-source modules in the phone are limited to what one would normally find in this kind of device.	Yealink phone firmware use some individual open source modules, such as the well-known openVPN, openLDAP, and mainstream VOIP phones in the industry will call and use these modules. Yealink lists more open source modules for your reference: https://www.yealink.com/open-source-software-yealink-phones
T54W Firmware Evaluation	We observed that the phone runs Linux kernel 4.9.75 (phone firmware version 96.84.30.0). We observed from open-source information (https://nvd.nist.gov/vuln/search/results?adv_search=true&isCpeNameSearch=true&query=cpe%3A2.3%3Ao%3Alinux%3Alinux_kernel%3A4.14.98%3A*%3A*%3A*%3A*%3A*%3A*%3A*) that there are many vulnerabilities in 4.14 but, in our opinion, only about 13 or 14 that apply to IP phones.	The Linux kernel is an open source software, and this version itself has security vulnerabilities, but Yealink has fixed and resolved key phone-related vulnerabilities during the secondary development process based on the open source kernel.
T54W Firmware Evaluation	Analysis of the firmware images showed them to have two main components: • ELF binary: version.bin • Unsorted Block Image (UBI) file: rfs.bin. Using Static Analysis, we observed that there are no signing requirements for firmware images read from disk, and no version checks that prevent downgrading firmware versions. Based on Static Analysis (Examination of the Firmware) of the current firmware version (96.84.30.0), we determined that the firmware images and filesystem blocks are encrypted with 4 possible ciphers: Cipher 3, Cipher 4, DES, and AES. Specifically, we observed that the images used what the manufacturer refers to as Cipher 3 for the protection of the data. We did not evaluate the runtime cryptography, as the filesystem of the firmware was not fully extracted. This phone, as designed and as the firmware is implemented, provides the ability for a malicious 3rd party, with access to the phone's network, to institute an attack on the customer.	Following the upgrade of technology, Yealink has continuously improved the security of the device in recent years, such as adding AES256, SHA256 and other encryption algorithms, which conform to the mainstream security standards and can ensure that software data packets cannot be forged from the source. During the software loading process, although the Yealink phone does not have a digital signature, the encrypted software needs to be verified by the security algorithm before the installation can be performed. This has the same security effect as the signature and can prevent the phone from loading tampered non-Yealink software.

T54W Hardware Evaluation	The main processor and NIC are sourced from Chinese suppliers (Rockchip YL2018G and Dongguan Mentech G4811CG, respectively). Flash memory and the display MCU are sourced from Taiwanese suppliers (Winbond 25N01GVZEIG and Holtek HT66F004, respectively). The Ethernet switch is sourced from a US company (Qualcomm QCA8334-AL3C), which appears from the markings on the packaging to be manufactured in Taiwan. In lieu of supply chain transparency, which is difficult to obtain in China, we assess the China-based parts and suppliers as "high risk" to US customers, particularly USG and critical infrastructure customers. We assess the Taiwan-based parts and suppliers as "moderate risk" given the dependencies those suppliers have on China overall.	All the Yealink products are all general civilian devices, and the chips and components used are all general device materials, which are not regulated or deemed unsafe.
T54W Hardware Evaluation	1. The main processor in the phone is Rockchip (model number YL2018G). It appears to be a custom Application Specific Integrated Circuit (ASIC) developed by Rockchip for Yealink. Rockchip is a national champion of the PRC for China based design of semiconductors. Vulnerabilities for ASICs do not get regularly reported in public vulnerability databases such as NIST's NVD data base. 2. Open-source information indicates that other Rockchip products have had vulnerabilities identified, both introduced by Rockchip at an individual product level as well as inherent in the ARM IP licensed by Rockchip. In the case of vulnerabilities from Arm IP, these vulnerabilities are common across many Arm licensees.	The chip used by Yealink is a general-purpose chip from OEM Rockchip. According to the information we know and the security report published by Rockchip, this chip has no risk or vulnerability.
Company Evaluation	This is based on Yealink's sources of Government financial support in the PRC, personnel in technical leadership positions and historical associations with foreign technical talent recruitment programs in China such as the Thousand Talents Program. 1. Yealink has obtained financial assistance from industrial programs that are sponsored by the government of the PRC. 2. Yealink has obtained PRC government assistance in recruiting technical talent from Silicon Valley. At least one current senior member of technical staff (Yang Gui) at Yealink has strong historic ties to PRC Government talent recruitment programs. These programs are focused on recruiting foreign-based technical talent to relocate to the PRC. The U.S. Government has assessed one of the programs to, "include provisions that violate U.S. standards for research integrity, place Thousand Talents Program	Yealink is not a state-owned enterprise, but a 100% listed company with no national background. All information is open to the public and can be checked at any time. Since its establishment, the company has always adhered to the principle of compliant operation, strictly abided by the laws and regulations of relevant countries and regions involved in production and operation activities, and has never had any business behaviors suspected of affecting user data security and technical security.

	members in compromising legal and ethical positions, and undermine fundamental U.S. scientific norms of transparency, reciprocity, and integrity” . This Yealink engineering executive is an Expert Committee Member of the China Ministry of Science and Technology.	

For further questions, please contact your Yealink representative or Yealink Data Security Compliance Officer via privacy@yealink.com