

## YEALINK IP PHONE – FIRMWARE UNPACKED ISSUE

### FIRMWARE UNPACKED ISSUE SUMMARY

The Yealink generic firmware & Lydis customized firmware of some of Yealink IP Phones (listed below) have a security issue of being unpacked. The main risk is that the built-in AutoProvision URL/username/password of the firmware package will be leaked. People who got the information can try to obtain the common.cfg file via auto provisioning, but cannot obtain the mac.cfg file.

The Yealink genetic firmware don't have customized URL information preset, but Lydis customized firmware is affected because it has auto provisioning code.

### Affected Yealink Model & Firmware

T4XS: T41S/T42S/T46S/T48S (EOL)	66.86.188.6 and prior
W80B	103.85.188.3 and prior
W60B (EOL)	77.85.188.5 and prior
W52P (EOL)	25.81.188.9 and prior
T58A,T56A (EOL)	58.86.188.2 and prior
CP960 (EOL)	73.86.188.1 and prior
CP920 (EOL)	78.85.188.2 and prior
T5XS: T52S/T54S (EOL)	70.83.188.9 and prior
T48G (EOL)	35.83.188.12 and prior
T46G (EOL)	28.83.188.12 and prior
T42G (EOL)	29.83.188.12 and prior
T41P (EOL)	36.83.188.11 and prior
T40G (EOL)	76.83.188.12 and prior
T40P (EOL)	54.83.188.11 and prior
T29G (EOL)	46.83.188.11 and prior
T27G (EOL)	69.85.188.6 and prior
T27P (EOL)	45.83.188.11 and prior
T23P,T23G (EOL)	44.83.188.12 and prior
T21PE2 (EOL)	52.83.188.11 and prior
T19PE2 (EOL)	53.83.188.11 and prior

### Yealink Recommended Solution

If you have one or more of the following security mechanisms in your AutoProvision server, you don't need to worry about the security risk caused by data leakage. Besides, Yealink has already released new firmware with new security mechanism, you could also plan to upgrade the firmware of phone.

- **IP Whitelist:** Your AutoProvision server can set IP whitelist, which can block requests from untrusted devices;

- **MAC/UA Authentication:** Your AutoProvision server can set MAC verification or UA (User Agent) verification. If the MAC or OUI (first 6 digits of MAC) of this device is not in your trust list, this device cannot download any configuration through auto provisioning.
- **Change the AutoProvision URL/username/password:** When you use the auto provisioning code, you may consider to change the authentication information. Please inform Yealink the new authentication information for the auto provisioning code feature, then Yealink will provide a new firmware. In this firmware, we have also added the new security mechanism. Afterwards, you can plan to upgrade the IP phone which deployed in the field and also change the authentication information in your AutoProvision server.
- If you have any question, please feel free to contact Lydis or [security&privacy@yealink.com](mailto:security&privacy@yealink.com)