CloudAware

Advisory - CVE-2022-48625

Title: Insecure RSA key in Yealink Configuration Encrypt Tool
Summary: A single, vendorwide, hardcoded RSA key in the configuration tool used to encrypt provisioning documents was leaked leading to a compromise of confidentiality of provisioning documents.
Date: 20-02-2024
Impact: information disclosure
Product: Yealink Configuration Encrypt Tool (RSA version <v1.2)

Solution: 1) Upgrade Yealink Configuration Encrypt Tool to version 1.2 or newer
2) Evaluate the impact of the disclosure of any configurations rolled out with prior versions of this tool (including, specifically, the leaking of passwords)

Mitigation: 1) If an upgrade is not an option - as `anyone' can create valid configuration files; ensure that affected equipment is unable to reach provisioning servers.
2) Evaluate the impact of the disclosure of any configurations rolled out prior to these mitigation steps

Detailed description:
The Yealink Configuration Encrypt Tool facilites provisioning and configuration mangement of Yealink products, such as VoIP phones. The tool created RSA encrypted provisioning documents, containing configuration directives such as

```
username=user1
passwword=passw0rd!
serverhost=sip.host.com
callerid=+19051231212
```

The files created by this tool are then transferred to the Yealink equipment. The equipment decrypts the files and uses them to configure itself.

This process needs to be secure. So these files are encrypted.

The key used to encrypt the provisioning document is encrypted by a hard-coded RSA private key and added to the provisioning document. This hard-coded RSA private key is identical across all installs and customers. After decryption of the encryption key, decryption of the confidential information, such as user passwords is trivial.

This implies that knowledge of this hardcoded RSA key allows for the disclosure of sensitive information from the configuration files, or that files with different information can be introduced and are axiomatically trusted by the phone.

As this key is static - this includes historic files from any customer that used this tool.

The vendor has fixed this in version 1.2 of the Configuration Encrypt Tool.

Weblinks:

- https://github.com/gitaware/CVE/tree/main/CVE-2022-48625
- https://github.com/gitaware/yealink-encryption
- https://cloudaware.eu/yealink/versleuteling/

History: early 2020, release of Configuration Encrypt Tool v1 containing RSA encryption method
august 2022, Yealink informed RSA key discovered and working in tool
2023, new version of Configuration Encrypt Tool v1.2 without a hardcoded RSA private key

Credit: Jeroen Hermans j.hermans[at]cloudaware.eu