CloudAware

Responsible Disclosure Document

Vulnerability type:	Hardcoded insecure key material
Vendor of the product:	Yealink
Product affected:	Yealink Configuration Encrypt Tool (AES version) Yealink Configuration Encrypt Tool (RSA version <v1.2)
Date:	01-02-2024
Impact:	Information disclosure
Affected components:	Yealink Configuration Encrypt Tool and all equipment using Yealink provisioning, incl. self-hosted
Attack vector:	Encrypted provisioning files can be decrypted using hardcoded, leaked AES key

Description:
The security mechanism of Yealink's Configuration Encrypt Tool relied on a single, hardcoded, AES key that has leaked. This hardcoded AES key was used in all equipment across installations/customers and product generations.

Access to this key compromises the supply/provisioning chain; allowing for the disclosure of sensitive (configuration) information such as passwords and for the introduction of data/configurations that may lead to an escalation of privelege or a DoS.

Discoverer:	Jeroen Hermans j.hermans[at]cloudaware.eu
References:	--

Bezuidenhoutseweg 98, NL-2594AZ Den Haag (NL)
T.: +31 (0)85 782 8878 E.: info@cloudaware.eu
KvK: 75426153