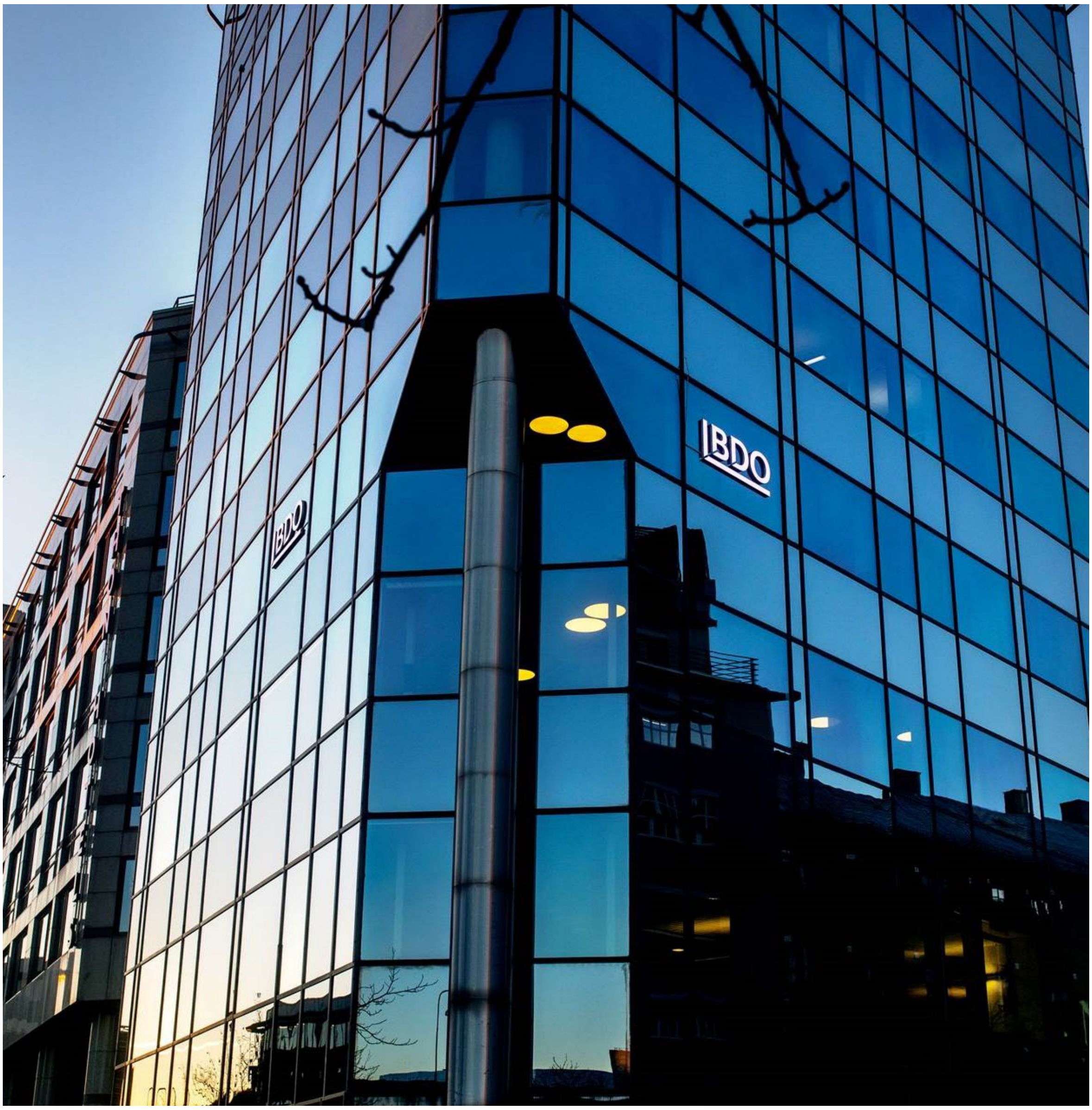

# EXECUTIVE SUMMARY: SECURITY EVALUATION OF THE YEALINK A10 MEETINGBAR AND CTP18 TOUCH PANEL

| | | |
|---|---|---|
| A10 FIRMWARE VERSION: | 278.320.0.53 | 30-10-2024 |
| CTP18 FIRMWARE VERSION: | 137.320.0.62 | |

This delivery has been prepared for the client and only covers the purposes agreed upon with them. Any other use and distribution is at the client's own expense and risk. BDO AS or BDO Advokater AS cannot be held liable to any third part

## 1. Evaluation Overview:

This report summarizes the findings of the security evaluation conducted on the A10 MeetingBar and CTP18 touch panel from Yealink. The evaluation encompassed multiple facets of security including network communication, web application integrity, and local system security. The devices were subjected to testing under various operational states including default (idle), during updates, and while actively engaged in meetings to simulate real-world usage and identify potential vulnerabilities.

## 2. Evaluation Methodology:

The testing methodology was designed to provide a comprehensive assessment of the devices' security capabilities. This included:

- PCAP Capture and Analysis:
  Monitoring and capturing network traffic to verify the security of DNS queries and network communications across different states of device operation.
- Network Penetration Testing:
  Utilizing tools such as Nmap and Nessus to conduct deep scans of the device's network ports to identify and test potential vulnerabilities.
- Web Application and API Analysis:
  Conducting security tests on the devices' web applications and APIs to identify vulnerabilities and assess the overall security posture of web-based services.
- File System and Process Access:
  Attempting to penetrate the device's local security measures to access file systems and process information, thereby evaluating the effectiveness of local device security.

## 3. Key Findings:

- Network Security:
  - The PCAP analysis confirmed that all DNS requests and server communications were properly registered with recognized organizations within the EU, the US, and an identified Australian server linked to Microsoft's update processes.
  - Network traffic was securely encrypted when appropriate, ensuring that data transfers during updates and Teams meetings were protected from interception and tampering.
- Network Penetration Testing:
  - Our testing of the devices' network ports revealed no vulnerabilities. The tests demonstrated that the devices' network interfaces were defended against unauthorized access attempts, with no exploitable vulnerabilities found in the open network ports.
- Web Application and API Security:
  - The security scans of the web applications and APIs running on the devices flagged two subjects for review. This was the .htaccess information and timestamp disclosure. After manual review it was concluded that no sensitive information was present. As these devices are not exposed as public-facing (internet-facing) services, we concluded that these are not security issues.
  - The overall security of the web applications and APIs was deemed robust, with no identified vulnerabilities which could be exploited.
- File System and Process Access:
  - The security measures in place effectively prevented any unauthorized access to the devices' file systems. Attempts to escalate privileges or access administrative

    - functions were unsuccessful, underscoring the effectiveness of the devices' security configurations.
    - The inability to access the file system or modify process information without appropriate credentials reflects positively on the security measures implemented by Yealink.

## 4. Conclusions and Recommendations:

The security evaluation of the A10 MeetingBar and the CTP18 Collaboration Touch Panel has demonstrated a high level of security across various testing categories. The devices exhibit robust defenses against potential network attacks, unauthorized access, and vulnerabilities within their web applications and APIs.

- Recommendations include:
    - Network Port Management: Continuously manage and monitor open network ports used for peripheral connectivity and perform regular assessments to proactively identify and mitigate potential vulnerabilities in future updates.

## 5. Overall Security Posture:

The A10 Meeting Bar and CTP18 Touch Panel demonstrate strong security postures. The implemented security measures offer robust protection against a broad spectrum of potential threats.

## CONTACT

Project Team:

Thomas Dahl
thomas.dahln@bdo.no
M: +47 916 60 057

Dashley Rouwendal van Schijndel
Dashley.vanschijndel@bdo.no
M: +47 407 52 412

BDO AS, a Norwegian registered company, is a participant in BDO International Limited, a UK company limited by guarantee, and is part of the international BDO network, which consists of independent firms in each country. Business register: NO 993 606 650 VAT. Member of the Norwegian Institute of Public Accountants.

This delivery has been prepared for the client and only covers the purposes agreed upon with them. Any other use and distribution is at the client's own expense and risk. BDO AS or BDO Advokater AS cannot be held liable to any third party