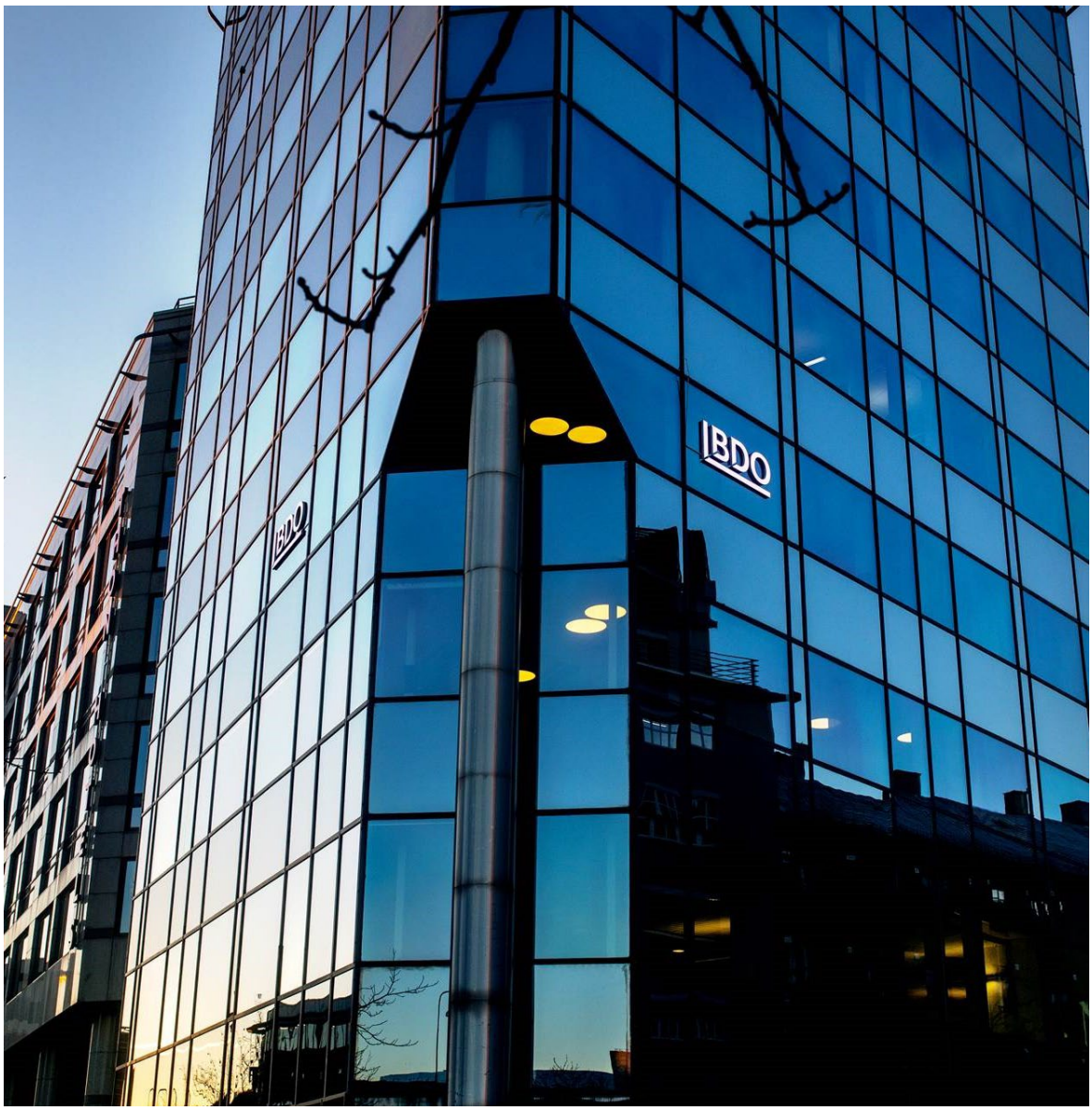

SECURITY EVALUATION EXECUTIVE SUMMARY – YEALINK MVC S40 SOLUTION

10-09-2024

1. Security Evaluation Methodology:

Our security evaluation targeted multiple assessments for verifying the MVC S40 Solution's integrity and security posture. We employed a diverse testing methodology, including PCAP capture and analysis, RAM capture and analysis, file system analysis, and network penetration testing. Each testing phase was designed to scrutinize the device's operational security under various conditions such as system updates, idle states, and active communication sessions via Microsoft Teams.

2. Objectives of the Evaluation:

The primary objective was to test and confirm the security robustness of the MVC S40 Solution. This involved ensuring that all network communications, software processes, and file systems adhered to the security standards required for secure operations. Our evaluation sought to identify any potential vulnerabilities that could be exploited in a real-world scenario and provide actionable recommendations to mitigate such risks.

3. Key Findings:

- **Network Security:**
    - Analysis of network traffic revealed that all DNS requests and server communications were securely managed. Network traffic during both the device updates and active Microsoft Teams meetings utilized appropriate encryption, ensuring secure data transmissions.
    - We confirmed that all server addresses and DNS requests were appropriately registered with recognized entities within the EU and the US, affirming the device's compliance with geographical and regulatory norms for data handling and privacy.
- **Software Integrity:**
    - Our RAM capture analysis identified several processes with elevated privileges, which were scrutinized for their origins and integrity. The majority of these processes were signed by trusted sources such as Microsoft and Yealink, indicating a high level of software security and authorization.
    - Two processes were unsigned; however, based on our observations combined with Microsoft's publicly available documentation we are convinced that these two process are legitimate software processes produced by Microsoft.
- **File System Security:**
    - We performed an exhaustive scan of the device's file system, which included comparing forensic copies made before and after software updates. This comparison helped us track changes and authenticate all modifications as legitimate and intentional.
    - No dangerous or unexplained alterations were detected in the file system. The software updates applied during the testing period were all accounted for and verified for their integrity and authenticity.

- **Network Penetration Testing:**

    - During the penetration tests, special attention was given to the device's network ports—a critical component for its functionality, especially in communicating with peripheral devices. The tests involved scanning these ports with advanced tools to identify any potential vulnerabilities.

    - Our findings indicated no security vulnerabilities in the open network ports. Despite the absence of immediate threats, the potential for future vulnerabilities exists, necessitating ongoing monitoring and updates to ensure the continued security of these critical points.

4. Conclusions and Recommendations:

The MVC S40 Solution has demonstrated comprehensive security across its network communications, software processes, and file system operations. The testing did not reveal any significant security flaws, affirming the device’s capability to function securely.

Given the dynamic nature of security threats, it is imperative that Yealink continues to monitor the security landscape and update the MVC S40 Solution accordingly. We recommend the following:

- **Continuous Monitoring:** Regularly update and patch software components to address new security vulnerabilities as they arise.

- **Process Verification:** Continue to ensure that all processes, especially those with elevated privileges, are verified, signed or documented to maintain system integrity.

- **Network Port Management:** To continue to security manage the open network ports used for peripheral connectivity, and conduct regular checks to preempt any exploitable vulnerabilities.

Additionally, we advise end-users to implement robust password management practices by changing default administrator credentials and employing complex password policies to safeguard local access to the devices.

CONTACT

Project Team:

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

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