Web Portal Vulnerabilities Updates: CVE-2020-12106, CVE-2020-12107

STATUS – RESOLVED
IMPACT – IMPORTANT

Executive Summary

The two flaws are found in the WiFi module's web portal which is an external module from the mobile encryptor. As a result, this could lead to unrestricted access to the device's WiFi functions or possible command injection via the web portal vulnerabilities.

Details

Please refer to the following details and impacts.
The flaws include critical web vulnerability that may lead to unrestricted access to several critical functions of the product's web portal and command injection vulnerability via the web portal leading to compromise of the device's OS. The extent of impact rest solely on WiFi functionalities and have no suspected security degradation to encryptor module. Extent of threat revolves primarily around denial of service through the Wifi module, affecting delivery of encrypted traffic.

CVE-2020-12106

The Web portal of the WiFi module of VPNCrypt M10 2.6.5 allows unauthenticated users to send HTTP POST request to several critical WiFi Administrative functions such as, changing credentials of the Administrator account or connect the product to a rogue access point.

CVE-2020-12107

The Web portal of the WiFi module of VPNCrypt M10 2.6.5 allows command injection via a text field, which allows full control over WiFi module's Operating System.

References

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12106
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12107

Impacted Products

The following product version is impacted:
VPNCrypt M10 (Version 2.6.5)

Updates for Affected Products

Product	Firmware Update
VPNCrypt M10	Version 2.6.6

Actions Required

The updated firmware with latest web portal versioning shall resolve the stated flaws. We strongly encourage users with affected product to upgrade the firmware. Possible means of upgrade will be sending back to the manufacturing house to perform the firmware upgrade.

Mitigations

VPNCrypt modular architecture protects the Encryptor's Host against threats from the WiFi module or any external devices or adversary. The Encryptor permits only authenticated traffic and shall block all illegitimate traffic delivered to it. With modules separation running separated operating systems (OS), compromisation of the WiFi module OS does not equate to a compromisation of the encryptor module. The Wifi module is an extension to VPNCrypt to allow wireless connectivity for delivery of encrypted traffic for purpose of mobility. Users can alternatively connect via the LAN port safely instead of the WiFi module to prevent any web portal compromise.