Apricorn - January 19, 2017

Configurator Security Assessment Customer Summary Letter

PRAETORIAN

OBJECTIVES & SCOPE

This document confirms the results of the recent security assessment undertaken by Apricorn and performed by Praetorian Group, Inc. The original assessment began on October 3, 2016, and concluded on October 14, 2016. The scope of work was defined as follows.

Scope of Work
Black-Box Penetration Test & Exploitation Analysis

• Security assessment of Apricorn's Configurator software and configuration process
  ○ Up to 5 different device models
  ▪ Examination of common set software only
  ○ Primary security analysis against software
  ○ Secondary security analysis against hardware
  ▪ Device emulation and firmware extraction
  ▪ Analysis narrowed to single model type
• Engagement evaluation activities will include:
  ○ Penetration testing and dynamic analysis
  ○ Reverse engineering and static analysis
  ○ Documentation and specification reviews
• Overall objective of the engagement will be to
  ○ Compromise configuration communications
  ○ Identify weaknesses in the configurator software
• Testing and exploitation techniques will include:
  ○ Device emulation attacks
  ○ Dynamic program analysis (e.g. fuzzing)
  ○ Static program analysis (e.g. taint analysis)
  ○ Combined methods (concolic and symbolic execution)
  ○ USB communication man-in-the-middle
• Comparison to SANS Top 25 List

Retests of the issues discovered during the initial test were performed on November 7 and 8, 2016, and January 18, 2017, in order to verify the effectiveness of Apricorn's remediations.

SECURITY ASSESSMENT RESULTS

The security assessment followed Praetorian's comprehensive methodology to provide a thorough analysis of the Configurator software. A security review of the hardware was also conducted, but was not the primary focus of the assessment. The shortcomings identified during the assessment were used to formulate recommendations and mitigation strategies for improving the overall security posture of the Configurator application. At the conclusion of the retests, the following numbers of findings remained.

Risk Rating	Findings Remaining
Critical	0
High	0
Medium	0
Low	0
Informational	2

CONCLUSION

Based on the evidence collected from the assessment cycle, Praetorian has concluded that the Configurator application exceeds "Industry Best Practice". That is to say, the application's overall security posture was found to be excellent, with no meaningful security risks detected.

Note that, as the application changes and as new vulnerabilities are made public, an application's overall security posture will change. Such changes will affect the validity of Praetorian's findings. Any statements made by Praetorian only describe a "snapshot" in time. Furthermore, as with all penetration tests, some vulnerabilities may not have been reported due to limitations in time, resources, and/or deltas between development and production environments.

PRAETORIAN