Samsung ARTIK Modules and Platform Software Engagement Summary

OWASP ASVS Level 1: Opportunistic Verification

Praetorian benchmarked the security posture of Samsung's ARTIK Cloud Platform against OWASP Application Security Verification Standard (ASVS) Level 1: Opportunistic.

Product Security Evaluation Performed by Independent Experts

This document confirms the results of the recent security evaluation undertaken by Samsung and performed by Praetorian. Between the dates of July 31, 2017 and September 1, 2017, Praetorian benchmarked the security posture of Samsung's ARTIK Cloud 053S and 530 Modules and Platform software against OWASP Application Security Verification Standard (ASVS) Level 1: Opportunistic. On the basis of that evaluation, Praetorian identified 0 Critical risk, 3 High risk, 2 Medium risk, 3 low risk, and 2 informational findings.

Between the dates of November 6, 2017 and November 13, 2017, Praetorian performed a retest of the findings discovered during the initial assessment to validate the effectiveness of Samsung's fixes. At the time of the retest, Praetorian identified 1 informational finding as present.

Based on the results of the retest, Praetorian assesses the overall security of ARTIK Modules and Platform software as excellent. The ARTIK Modules and Platform software meet the requirements of OWASP ASVS Level 1 and have adequate security controls in place to defend against security vulnerabilities that are easy to discover.

As the Samsung ARTIK Modules and Platform software continue to change, so too will it's overall security posture. Such changes will affect the validity of Praetorian's findings and this letter. Therefore, any statements made by Praetorian only describe a "snapshot" in time. Praetorian would like to thank Samsung for this opportunity to help the organization evaluate its current security posture.

Issued date
NOVEMBER 17, 2017

Valid until
NOVEMBER 16, 2018

Nathan Sportsman
Chief Executive Officer, Praetorian
nathan.sportsman@praetorian.com
(512) 410-0350 Phone
(512) 410-0356. Fax

Praetorian assesses that ARTIK Modules and Platform software meet the requirements of OWASP ASVS Level 1 and have adequate security controls in place to defend against security vulnerabilities that are easy to discover.

OWASP ASVS Certification Level

OWASP ASVS is a list of application security requirements or tests that can be used by architects, developers, testers, security professionals, and even consumers to define what a secure application is. Evaluation ratings compare information gathered during the course of the engagement to the OWASP ASVS version 3.1[1] criteria for security standards.

Product	Verification Level
Samsung ARTIK Cloud Platform and SDK	**OWASP Level 1: Opportunistic**

OWASP ASVS Level	Criteria Description
Level 3: Advanced	An application achieves Level 3 (or Advanced) certification if it also adequately defends against all advanced application security vulnerabilities, and also demonstrates principles of good security design.
Level 2: Standard	An application achieves Level 2 (or Standard) verification if it also adequately defends against prevalent application security vulnerabilities whose existence poses moderate-to-serious risk.
Level 1: Opportunistic	An application achieves Level 1 (or Opportunistic) certification if it adequately defends against application security vulnerabilities that are easy to discover.
Level 0: Cursory	Level 0 (or Cursory) is an optional certification, indicating that the application has passed some type of verification.

Praetorian Grading Report Card

The grade below is a representation of Samsung's ARTIK Modules and Platform software's current, post-remediation security posture. Praetorian calculates grades based on the "Existing Vulnerability Measure" (EVM) formula described in the reference below[2]. EVM is used to quantify the collective risk of the findings identified during this assessment. The letter grade leverages EVM to benchmark risk posture against Praetorian's client-base.

Product	Security	Grade
Samsung ARTIK 053S and 530 Modules and Platform Software	**Excellent**	**A**

Grade	Security	Criteria Description
A	**Excellent**	The EVM of the assessed components placed within the top 5-10% of Praetorian's client-base. The overall security posture was found to be excellent with a minimal amount of low and informational risk findings identified.
B	**Good**	The EVM of the assessed components was above average when benchmarked against Praetorian's client-base. Only a handful of low/informational risk shortcomings were identified in the testing time period.
C	**Fair**	The EVM of the assessed components was aligned closely to the average EVM of Praetorian's client-base. The current solutions protect some areas of the target from security issues, but moderate changes are required to elevate the discussed areas to acceptable standards.
D	**Poor**	The EVM of the assessed components fell below the average EVM, with significant security deficiencies present. Immediate attention should be given to the discussed issues to address exposures identified.
F	**Inadequate**	Serious security deficiencies were present in the assessed components and the EVM placed within the bottom 5-10% of Praetorian's client-base. Shortcomings were identified throughout most of the security controls examined and improved security will require significant resources.

[1] https://github.com/OWASP/ASVS/blob/master/OWASP Application Security Verification Standard 3.1.pdf

[2] https://dl.acm.org/citation.cfm?id=1179505

Samsung ARTIK™

Praetorian's OWASP ASVS assessment requires the vendor to remediate all critical, high, medium, and low risk severity findings within 90-days.

In total, OWASP ASVS contains 17 unique security control category requirements. OWASP ASVS detailed verification requirements and the vulnerabilities discovered during Praetorian's first and second security assessment are shown in the tables to the right.

The top table provides an overview of findings found during the initial assessment.

The bottom table showcases findings Praetorian identified following active remediation efforts, which took place during the course of the initial assessment and continued following its completion for a period not exceeding 90-days.

Guided by OWASP Application Security Verification Standard (ASVS)

ASVS Categorization of Findings Discovered by Praetorian

Security Control Category	Findings as of September 1, 2017					Total
	Critical	High	Medium	Low	Info	
Architecture, design and threat modeling	-	-	-	-	-	-
Authentication	-	3	1	-	-	4
Session management	-	-	-	-	-	-
Access control	-	-	-	-	-	-
Malicious input handling	-	-	-	-	1	1
Cryptography at rest	-	-	-	2	1	3
Error handling and logging	-	-	-	-	-	-
Data protection	-	-	-	-	-	-
Communications	-	-	-	-	-	-
HTTP security configuration	-	-	-	-	-	-
Malicious controls	-	-	-	-	-	-
Business logic	-	-	-	-	-	-
File and resources	-	-	-	-	-	-
Mobile	-	-	-	-	-	-
Web services	-	-	-	-	-	-
Configuration	-	-	-	-	-	-
Device hardware	-	-	1	1	-	2
Total	**0**	**3**	**2**	**3**	**2**	**10**

LESS THAN 90-DAY ACTIVE REMEDIATION

Security Control Category	Findings as of November 13, 2017					Total
	Critical	High	Medium	Low	Info	
Architecture, design and threat modeling	-	-	-	-	-	-
Authentication	-	-	-	-	-	-
Session management	-	-	-	-		-
Access control	-	-	-	-	-	-
Malicious input handling	-	-	-	-	-	-
Cryptography at rest	-	-	-	-	-	-
Error handling and logging	-	-	-	-	-	-
Data protection	-	-	-	-	1	1
Communications	-	-	-	-	-	-
HTTP security configuration	-	-	-	-	-	-
Malicious controls	-	-	-	-	-	-
Business logic	-	-	-	-	-	-
File and resources	-	-	-	-	-	-
Mobile	-	-	-	-	-	-
Web services	-	-	-	-	-	-
Configuration	-	-	-	-	-	-
Device hardware	-	-	-	-	-	-
Total	-	-	-	-	1	1

