**National Information Assurance Partnership**

**Common Criteria Evaluation and Validation Scheme**



®

**TM**

**Validation Report**

**Application Software Extended Package for Web Browsers, Version 2.0, 16 June 2015**

**Report Number: CCEVS-VR-PP-0059**

**Dated: 3 December 2018**

**Version: 1.0**

|  |  |  |  |
| --- | --- | --- | --- |
| **National Institute of Standards and Technology** | |  | **National Security Agency**  **Information Assurance Directorate**  **9800 Savage Road STE 6940**  **Fort George G. Meade, MD 20755-6940** |
| **Information Technology Laboratory**  **100 Bureau Drive**  **Gaithersburg, MD 20899** |  |

**ACKNOWLEDGEMENTS**

**Common Criteria Testing Laboratory**

***Base Requirements***

*Acumen Security Common Criteria Testing Laboratory*

*Rockville, Maryland*

**Table of Contents**

[1 Executive Summary 1](#_Toc531597087)

[2 Identification 1](#_Toc531597088)

[3 WBEP Description 2](#_Toc531597089)

[4 Security Problem Description and Objectives 2](#_Toc531597090)

[4.1 Assumptions 2](#_Toc531597091)

[4.2 Threats 3](#_Toc531597092)

[4.3 Organizational Security Policies 3](#_Toc531597093)

[4.4 Security Objectives 3](#_Toc531597094)

[5 Requirements 4](#_Toc531597095)

[6 Assurance Requirements 5](#_Toc531597096)

[7 Results of the Evaluation 6](#_Toc531597097)

[8 Glossary 6](#_Toc531597098)

[9 Bibliography 7](#_Toc531597099)

# Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Application Software Extended Package for Web Browsers, version 2.0 (WBEP), which extends the Protection Profile for Application Software (App PP). It presents a summary of the WBEP and the evaluation results.

Acumen performed the evaluation of the WBEP concurrent with the first product evaluation against the Extended Package’s (EP’s) requirements. In this case the Target of Evaluation (TOE), Apple iOS 11 Safari, evaluated by Acumen Security in Rockville, MD, United States of America.

This evaluation addressed the base requirements of the WBEP. The WBEP also includes several optional, selection-based, and objective requirements; however, the evaluated TOE did not include any this functionality, so they were not claimed by this evaluation.

The Validation Report (VR) author independently performed an additional review of the EP as part of the completion of this VR, to confirm it meets the claimed APE assurance requirements.

The evaluation determined the WBEP is both Common Criteria Part 2 Extended and Part 3 Conformant. A NIAP approved CCTL evaluated the EP identified in this VR using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). The Security Target (ST) includes material from both the App PP and the WBEP; completion of the ASE work units satisfied the APE work units for this EP, but only for the materials defined in this EP.

The evaluation laboratory conducted this evaluation in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS). The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence given.

# Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called CCTLs. CCTLs evaluate products against Protection Profiles (PPs) and EPs that have Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP or EP.

In order to promote thoroughness and efficiency, the evaluation of the WBEP was performed concurrent with the first product evaluation against the EP’s requirements. In this case the Target of Evaluation (TOE) was Apple iOS 11 Safari, performed by Acumen Security in Rockville, MD, United States of America.

The WBEP has a set of “base” requirements all conformant STs must include and also has “Optional,” “Selection-based,” and “Objective” requirements. Optional requirements define functionality subjected to security evaluation that not all conformant TOEs need to include. Selection-based requirements must be included based on the selections made in the base requirements and the capabilities of the TOE. Objective requirements are those the EP sponsor intends to mandate in future versions and are included as optional requirements that raise industry awareness of expected future requirements. This evaluation did not claim the functions these requirements described.

A specific ST may not include these discretionary requirements, so the initial use of the EP addresses (in terms of the EP evaluation) the base requirements and any additional requirements incorporated into the initial ST. The VR authors have evaluated all discretionary requirements that were not claimed in the initial TOE evaluation as part of the evaluation of the APE\_REQ work units performed against the ESCP. When an evaluation laboratory evaluates a TOE against any additional requirements not already referenced in this VR through an existing TOE evaluation, the VR may be amended to include reference to this as additional evidence that the corresponding portions of the WBEP were evaluated.

The following identifies the EP that is evaluated by this VR. It also includes supporting information from the initial product evaluation performed against this EP and any subsequent evaluations that address additional optional, selection-based, or objective requirements in the WBEP.

|  |  |
| --- | --- |
| **Protection Profile/Extended Package** | Application Software Extended Package for Web Browsers, Version 2.0, 16 June 2015 |
| **ST (Base)** | Apple iOS 11 Safari Security Target, Version 1.0, November 2018 |
| **Assurance Activity Report (Base)** | Common Criteria SWAPP and WEBBROWSEREP Assurance Activity Report Apple iOS 11 Safari, Version 0.5, November 2018 |
| **CC Version** | Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4 |
| **Conformance Result** | CC Part 2 Extended, CC Part 3 Conformant |
| **CCTL** | Acumen Security, Rockville, MD, USA |

# WBEP Description

The WBEP specifies information security requirements for enterprise session controllers, as well as the assumptions, threats, organizational security policies, objectives, and requirements of a compliant TOE.

A web browser in the context of this EP is a client application that retrieves and renders content supplied by web servers, primarily using the hypertext transfer protocol (HTTP) or HTTP Secure (HTTPS).

# Security Problem Description and Objectives

## Assumptions

The specific conditions listed in the following subsections should exist in the TOE’s Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

**Table 1: Assumptions**

|  |  |
| --- | --- |
| **Assumption Name** | **Assumption Definition** |
| This EP does not define any assumptions. | |

## Threats

The following table shows applicable threats, in addition to those defined in the App PP.

**Table 2: Threats**

|  |  |
| --- | --- |
| **Threat Name** | **Threat Definition** |
| T.FLAWED\_ADDON | Web browser functionality can be extended through the integration of third­-party utilities and tools. Malicious or vulnerable add­-ons could result in attacks against the system. Such attacks can allow unauthorized access to sensitive information in the browser, unauthorized access to the platform's file system, or even privilege escalation that enables unauthorized access to other applications or the operating system. |
| T.SAME-ORIGIN\_VIOLATION | Violating the same­-origin policy is a specialized type of network attack (covered generally as T.NETWORK\_ATTACK in the App PP) which involves web content violating access control policies enforced by a web browser to separate the content of different web domains. It is specifically identified as a threat to web browsers, since they implement the access control policies that are violated in these attacks. |

## Organizational Security Policies

The following table shows applicable organizational security policies, in addition to those defined in the App PP.

**Table 3: Organizational Security Policies**

|  |  |
| --- | --- |
| **OSP Name** | **OSP Definition** |
| This EP does not define any organizational security policies. | |

## Security Objectives

The following table shows security objectives for the TOE, in addition to those defined in the App PP. Note also that some SFRs in the WBEP are used to further satisfy objectives defined in the App PP for behavior that is unique to this specific type of application.

**Table 4: Security Objectives for the TOE**

| **TOE Security Obj.** | **TOE Security Objective Definition** |
| --- | --- |
| O.DOMAIN\_ISOLATION | To address the network attack associated with content leakage between different web domains, the browser must ensure that content originating from different domains (e.g., in a tab or iFrame) is properly isolated. |
| O.ADDON\_INTEGRITY | To address issues associated with malicious or flawed add­-ons, conformant browsers implement mechanisms to ensure their integrity. This includes verification and validation at installation time and update. |

The following table shows security objectives for the Operational Environment, in addition to those defined in the App PP.

**Table 5: Security Objectives for the Operational Environment**

|  |  |
| --- | --- |
| **Environmental Security Objective** | **Environmental Security Objective Definition** |
| This EP does not define environmental security objectives. The App PP that this EP extends defines all relevant environmental objectives. | |

# Requirements

As indicated above, the WBEP requirements include the “base” requirements and additional requirements that are strictly or conditionally optional. The following table shows the “base” requirements validated as part of the Apple evaluation activities referenced above.

**Table 6: Base Requirements**

|  |  |  |
| --- | --- | --- |
| **Requirement Class** | **Requirement Component** | **Verified By** |
| **FDP: User Data Protection** | FDP\_ACF\_EXT.1 Local and Session Storage Separation | iOS 11 Safari |
| FDP\_COO\_EXT.1 Cookie Blocking | iOS 11 Safari |
| FDP\_SBX\_EXT.1 Sandboxing of Rendering Processes | iOS 11 Safari |
| FDP\_SOP\_EXT.1 Same Origin Policy | iOS 11 Safari |
| FDP\_STR\_EXT.1 Secure Transmission of Cookie Data | iOS 11 Safari |
| FDP\_TRK\_EXT.1 Tracking Information Collection | iOS 11 Safari |
| **FMT: Security Management** | FMT\_MOF\_EXT.1 Management of Functions Behavior | iOS 11 Safari |
| **FPT: Protection of the TSF** | FPT\_DNL\_EXT.1 File Downloads | iOS 11 Safari |
| FPT\_MCD\_EXT.1 Mobile Code | iOS 11 Safari |
| FPT\_AON\_EXT.1 Support for Only Trusted Add-ons | iOS 11 Safari |

The following table shows the “**Optional**” requirements included in Appendix A, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are found in an ST if the ST authors claim that the TOE includes one or more of these optional capabilities.

**Table 7: Optional Requirements**

|  |  |  |
| --- | --- | --- |
| **Requirement Class** | **Requirement Component** | **Verified By** |
| **FDP: User Data Protection** | FDP\_PST\_EXT.1 Storage of Persistent Information | PP Evaluation |

The following table shows the “**Selection-Based**” requirements included in Appendix B, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are found in an ST if the ST authors make associated selections in requirements levied on the TOE by the ST.

**Table 8: Selection-Based Requirements**

|  |  |  |
| --- | --- | --- |
| **Requirement Class** | **Requirement Component** | **Verified By** |
| **FPT: Protection of the TSF** | FPT\_AON\_EXT.2 Trusted Installation and Update for Add-Ons | PP Evaluation |

The following table shows the “**Objective**” requirements included in Appendix B, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are found in an ST if the ST authors claim that the TOE includes one or more of these optional capabilities.

**Table 9: Objective Requirements**

|  |  |  |
| --- | --- | --- |
| **Requirement Class** | **Requirement Component** | **Verified By** |
| **FCS: Cryptographic Support** | FCS\_STS\_EXT.1 Strict Transport Security | PP Evaluation |
| **FPT: Protection of the TSF** | FPT\_INT\_EXT.1 Interactions with Application Reputation Services | PP Evaluation |
| FPT\_INT\_EXT.2 Interactions with URL Reputation Services | PP Evaluation |

# Assurance Requirements

The following shows the assurance requirements included in the WBEP.

**Table 10: Assurance Requirements**

| **Requirement Class** | **Requirement Component** | **Verified By** |
| --- | --- | --- |
| **ASE: Security Target** | ASE\_CCL.1: Conformance Claims | iOS 11 Safari |
| ASE\_ECD.1: Extended Components Definition | iOS 11 Safari |
| ASE\_INT.1: ST Introduction | iOS 11 Safari |
| ASE\_OBJ.2: Security Objectives | iOS 11 Safari |
| ASE\_REQ.2: Derived Security Requirements | iOS 11 Safari |
| ASE\_SPD.1: Security Problem Definition | iOS 11 Safari |
| ASE\_TSS.1: TOE Summary Specification | iOS 11 Safari |
| **ADV:**  **Development** | ADV\_FSP.1 Basic Functional Specification | iOS 11 Safari |
| **AGD: Guidance Documents** | AGD\_OPE.1: Operational User Guidance | iOS 11 Safari |
| AGD\_PRE.1: Preparative Procedures | iOS 11 Safari |
| **ALC: Life-cycle Support** | ALC\_CMC.1: Labeling of the TOE | iOS 11 Safari |
| ALC\_CMS.1: TOE CM Coverage | iOS 11 Safari |
| **ATE: Tests** | ATE\_IND.1: Independent Testing - Sample | iOS 11 Safari |
| **AVA: Vulnerability Assessment** | AVA\_VAN.1: Vulnerability Survey | iOS 11 Safari |

# Results of the Evaluation

Note that for APE elements and work units identical to ASE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

**Table 11: Evaluation Results**

|  |  |  |
| --- | --- | --- |
| **APE Requirement** | **Evaluation Verdict** | **Verified By** |
| **APE\_CCL.1** | Pass | iOS 11 Safari |
| **APE\_ECD.1** | Pass | iOS 11 Safari |
| **APE\_INT.1** | Pass | iOS 11 Safari |
| **APE\_OBJ.2** | Pass | iOS 11 Safari |
| **APE\_REQ.2** | Pass | iOS 11 Safari |
| **APE\_SPD.1** | Pass | iOS 11 Safari |

# Glossary

The following definitions are used throughout this document:

* **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
* **Conformance**. The ability to demonstrate unambiguously that a given implementation is correct with respect to the formal model.
* **Evaluation**. An IT product’s assessment against the Common Criteria using the Common Criteria Evaluation Methodology as the supplemental guidance, interprets it in the WBEP Assurance Activities to determine whether the claims made are justified.
* **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
* **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
* **Validation**. The process the CCEVS Validation Body uses that leads to the issuance of a Common Criteria certificate.
* **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

# Bibliography

The validation team used the following documents to produce this VR:

1. Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 4, dated: September 2012.
2. Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 4, dated: September 2012.
3. Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 4, dated: September 2012.
4. Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 4, dated: September 2012.
5. Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 3.0, May 2014.
6. Application Software Extended Package for Web Browsers, Version 2.0, 16 June 2015
7. Protection Profile for Application Software, Version 1.2, 22 April 2016
8. Apple iOS 11 Safari Security Target, Version 1.0, November 2018
9. Common Criteria SWAPP and WEBBROWSEREP Assurance Activity Report Apple iOS 11 Safari, Version 0.5, November 2018