Эшелон
комплексная безопасность

АКЦИОНЕРНОЕ ОБЩЕСТВО
«НАУЧНО-ПРОИЗВОДСТВЕННОЕ ОБЪЕДИНЕНИЕ «ЭШЕЛОН»

УТВЕРЖДАЮ
Генеральный директор
АО «НПО «Эшелон»
_____ В.Цирлов
«___» _____ 2021 г.
М.П.

ТЕХНИЧЕСКОЕ ЗАКЛЮЧЕНИЕ

по результатам проведения работ по оценке соответствия изделия «Система Дистанционного Банковского Обслуживания «UBS.NET» ВЕРСИЯ RB_124» требованиям ГОСТ Р ИСО/МЭК 15408-3-2013 по оценочному уровню доверия 4 и по проведению анализа уязвимостей

ИЦ-ЭШ.004-21/СтБИ ТЗ

Листов 8

Москва
2021

Содержание

1 Общие положения

В настоящем документе отражены общие результаты и выводы, полученные при проведении работ по оценке соответствия изделия «Система Дистанционного Банковского Обслуживания «UBS.NET» ВЕРСИЯ RB_124», включающая: «UBS-Home, Физические лица» (web-интерфейс, мобильное приложение платформы IOS, Android), «UBS-Office, Юридические лица» (web-интерфейс), «UBS - серверная часть» требованиям ГОСТ Р ИСО/МЭК 15408-3-2013 по оценочному уровню доверия 4 и по проведению анализа уязвимостей.

Заказчик: ООО «ЮБС» (юридический адрес: 129329, г Москва, улица Ивовая, 1к1, тел. +7 495 741-45-35).

Исполнитель: Испытательная лаборатория АО «НПО «Эшелон» (юридический адрес: 107023, г. Москва, ул. Электрозаводская, д. 24, тел. 8 (495) 223-23-92).

2 Цель проведения испытаний

Испытания проводились с целью поиска уязвимостей в оцениваемом изделии, с целью оценки соответствия изделия «Система Дистанционного Банковского Обслуживания «UBS.NET» требованиям ГОСТ Р ИСО/МЭК 15408-3-2013 по оценочному уровню доверия 4, а также с целью проведения анализа уязвимостей в соответствии с требованиями ГОСТ Р ИСО/МЭК 15408-3-2013. При проведении анализа уязвимостей проводился:

- анализ изделия на предмет наличия актуальных угроз безопасности и программных закладок:
  - методом серого ящика;
  - методом белого ящика.
- анализ кода изделия и дополнительно подключаемых модулей;
- выявление недостатков в применяемых Заказчиком мерах информационной безопасности и оценка возможности их использования нарушителем;
- анализ корректности взаимодействия подключаемых к приложению сторонних модулей. Анализ корректности взаимодействия приложения с сторонними информационными ресурсами;
- выявление уязвимостей и программных закладок на основе проведённого анализа составных частей приложения;
- проверка корректности внедрения применяемых технологий защиты информации.

При проведении оценки соответствия эксперт исследовал документацию на изделие, а также проводил тестирование изделия.

3 Результаты проведения исследований

В ходе выполнения исследований в части проведения анализа уязвимостей были выявлены недостатки, описание которых представлено в таблице 1 далее по тексту. Выявленные недостатки позволяют обходить штатные механизмы защиты. В ходе анализа сторонних модулей выявить влияние работы этих модулей на механизмы защиты объекта оценки (далее по тексту - ОО) не удалось. Испытательная лаборатория установила, что разработчик доработал изделие с целью устранения выявленных недостатков. При повторном проведении оценки новых уязвимостей выявлено не было.

Таблица 1 – Описание полученных результатов по результатам проведения анализа уязвимостей

Идент. недост.	Краткое описание результатов	Заключение ИЛ
VUL_P1	Потенциальная уязвимость, связанная с возможностью получения отказа в обслуживании	Уязвимость, актуальная для ОО. После взаимодействия с разработчиком уязвимость была устранена.
VUL_P2	Потенциальная уязвимость, связанная с некорректной обработкой запросов	Уязвимость, актуальная для ОО. После взаимодействия с разработчиком уязвимость была устранена.
VUL_P3	Потенциальная уязвимость, позволяющая злоумышленнику с доступом к учетной записи с любой ролью получать, создавать, модифицировать и удалять конфиденциальные данные, после удаления данного пользователя из системы, до момента окончания его текущей сессии.	Уязвимость, актуальная для ОО. После взаимодействия с разработчиком уязвимость была устранена.
VUL_P4	Потенциальная уязвимость, связанная с обходом механизма аутентификации	Уязвимость, актуальная для ОО. После взаимодействия с разработчиком уязвимость была устранена.
VUL_P5	Потенциальная уязвимость, связанная с отсутствием корректной обработки программным кодом данных, используемых для генерации веб-страниц, возвращаемых пользователю, что приводит к успешной атаке типа «межсайтовое выполнение скриптов».	Уязвимость, актуальная для ОО. После взаимодействия с разработчиком уязвимость была устранена.
VUL_P6	Потенциальная уязвимость, позволяющая злоумышленнику перенаправлять с уязвимого доверенного веб-приложения на фишинговый/недоверенный сайт, с целью хищения данных или иных	Уязвимость, актуальная для ОО. После взаимодействия с разработчиком уязвимость была устранена.

	намерений, путем встраивания вредоносной ссылки в поле ввода.	

При проведении оценки соответствия изделия «Система Дистанционного Банковского Обслуживания «UBS.NET» требованиям ГОСТ Р ИСО/МЭК 15408-3-2013 по оценочному уровню доверия 4 были получены результаты, представленные в таблице далее по тексту. В ходе испытаний было установлено соответствие изделия требованиям ГОСТ Р ИСО/МЭК 15408-3-2013 по оценочному уровню доверия 4. При проведении функционального тестирования было установлено соответствие информации, представленной в документации, результатам, полученным в ходе функционального тестирования.

Таблица 2 – Описание полученных результатов оценки соответствия изделия требованиям ГОСТ Р ИСО/МЭК 15408-3-2013[1]

Класс	**Компонент доверия**	**Действие оценщика**	**Вердикт**		
			Действие оценщика	**Компонент доверия**	**Класс**
ADV	ADV_ARC.1	ADV_ARC.1.1E	+	+	+
	ADV_FSP.4	ADV_FSP.4.1E	+	+	
		ADV_FSP.4.2E	+		
	ADV_IMP.2	ADV_IMP.2.1E	+	+	
		ADV_IMP.2.2E	+		
	ADV_TDS.3	ADV_TDS.3.1E	+	+	
		ADV_TDS.3.2E	+		
ALC	ALC_CMC.4	ALC_CMC.4.1E	+	+	+
	ALC_CMS.4	ALC_CMS.4.1E	+	+	
	ALC_DEL.1	ALC_DEL.1.1E	+	+	
		ALC_DEL.1.2D	+		
	ALC_DVS.1	ALC_DVS.1.1E	+	+	
		ALC_DVS.1.2E	+		
	ALC_LCD.1	ALC_LCD.1.1E	+	+	
	ALC_TAT.1	ALC_TAT.1.1E	+	+	
AGD	AGD_OPE.1	AGD_OPE.1.1E	+	+	+
	AGD_PRE.1	AGD_PRE.1.1E	+	+	
		AGD_PRE.1.2E	+		
ATE	ATE_COV.2	ATE_COV.2.1E	+	+	+

[1] (+) – положительный вердикт, вынесенный оценщиком, (-) – соответствие не установлено

Класс	Компонент доверия	Действие оценщика	Вердикт		
			Действие оценщика	Компонент доверия	Класс
	ATE_DPT.2	ATE_DPT.1.1E	+	+	
	ATE_FUN.1	ATE_FUN.1.1E	+	+	
	ATE_IND.2	ATE_IND.2.1E	+	+	
		ATE_IND.2.2E	+		
		ATE_IND.2.3E	+		
AVA_VAN	AVA_VAN.5	AVA_VAN.5.1E	+	+	+
		AVA_VAN.5.2E	+		
		AVA_VAN.5.3E	+	+	
		AVA_VAN.5.4E	+		

4 Выводы по результатам проведения исследований

Испытательной лабораторией был установлен факт наличия возможностей, используя которые злоумышленник может воздействовать на конфиденциальность, целостность и доступность информации. После устранения выявленных дефектов Испытательной лабораторией новых дефектов обнаружено не было. ОО соответствует требованиям ГОСТ Р ИСО/МЭК 15408-3-2013 по оценочному уровню доверия 4. В ходе исследования документации на изделие было установлено, что изделие разработано в соответствии с требованиями ГОСТ Р 56939-2016.

Эксперт испытательной лаборатории:

С. Арустамян