ПромСвязьИнвест
расчетная небанковская кредитная организация
367000 РФ, Республика Дагестан, г. Махачкала, ул. Ирчи-Казака 2 «б»
ОКПО 43340114 БИК № 048209395 корсчет 30103810982090000395
тел.(8722) 62-16-24, 61-58-22 факс.(8722) 62-16-94 www.psib.ru E-mail: office@psib.ru

«01» сентября 2023г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за август 2023 г.»

В связи с необходимостью снижения рисков воздействия вредоносного кода, рисков использования уязвимостей программного обеспечения и повышения уровня защиты информации при работе с системой дистанционного банковского обслуживания «iBank2» (Интернет-банком) служба информационной безопасности РНКО «ПРОМСВЯЗЬИНВЕСТ» (ООО) рекомендует it-специалистам наших клиентов (организаций и индивидуальных предпринимателей) применять в своей работе рекомендации по защите информации, указанные в Приложении 1 к данному письму. В случае возникновения вопросов по применению рекомендаций просим Вас позвонить в службу информационной безопасности по номерам 8(8722) 51-70-44 или направить письмо по электронной почте office@psib.ru .

Председатель Правления _____ **Абдурахманов К.А.**
подпись

Приложение № 1
к информационному письму
«Информирование клиентов системы
дистанционного банковского
обслуживания «iBank2» о мерах
защиты за август 2023 г.»

На компьютере, с использованием которого осуществляется работа в системе ДБО «iBank2», не рекомендуется устанавливать программное обеспечение, имеющее уязвимости с критичным уровнем опасности. К такому программному обеспечению относится программное обеспечение, указанное в таблице ниже:

№	Наименование уязвимого программного Обеспечения	Идентификатор уязвимостей	Описание уязвимости	Дата выявления	Ссылка на источники	Наличие обновлений
	Выполнение произвольного кода в Ubuntu	CVE-2023-35001	Выполнение произвольного кода. Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	2023-07-26	http://ubuntu.com/security/notices/USN-6250-1 https://bdu.fstec.ru/vul/2023-03778	Есть
	Повышение привилегий в Ubuntu	CVE-2023-3390	Повышение привилегий. Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	2023-07-26	http://ubuntu.com/security/notices/USN-6250-1 https://bdu.fstec.ru/vul/2023-03677	Есть
	Повышение привилегий в MikroTik RouterOS	CVE-2023-30799	Повышение привилегий. Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	2023-07-27	http://vulncheck.com/advisories/mikrotik-foisted • http://github.com/MarginResearch/FOISted • https://bdu.fstec.ru/vul/2023-04167	Есть
	Выполнение произвольного кода в Foxit PDF Editor и Reader для Mac	CVE-2023-28744	Выполнение произвольного кода. Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления	2023-07-26	http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+for+Mac+12.1.1+and+Foxit+PDF+Reader+for+Mac+12.1.12023-07-25+00%3A00%3A00	Есть

			программного обеспечения только после оценки всех сопутствующих рисков.			
	Получение конфиденциальной информации в Microsoft Edge	CVE-2023-38187	Получение конфиденциальной информации. Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	2023-07-22	http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38187	Есть
	Отказ в обслуживании в Microsoft Edge	CVE-2023-3740	Отказ в обслуживании. Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	2023-07-22	http://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-3740	Есть
	Пользовательский интерфейс подмены в Microsoft Edge	CVE-2023-3734	Пользовательский интерфейс подмены. Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	2023-07-22	http://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-3734	Есть
	Повышение привилегий в Zoom Desktop Client для Windows	Повышение привилегий в Zoom Desktop Client для Windows CVE-2023-36534	Повышение привилегий. Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	2023-08-08	https://exchange.xforce.ibmcloud.com/vulnerabilities/262825	Есть
	Выполнение произвольного кода в 7-Zip	CVE-2023-40481	Выполнение произвольного кода. Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем	2023-08-25	http://www.zerodayinitiative.com/advisories/ZDI-23-1164/ • http://sourceforge.net/p/sevenzip/discussion/45797/thread/713c8a8269/ • https://bdu.fstec.ru/vul/2023-04886	Есть

			устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.			
	Выполнение произвольного кода в ASUS RT-AX56U V2 и RT-AC86U	CVE-2023-35086	Выполнение произвольного кода. Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	2023-07-21	https://nvd.nist.gov/vuln/detail/CVE-2023-35086 • https://bdu.fstec.ru/vul/2023-04333	Есть
	Отказ в обслуживании в TP-LINK Archer C50v2 Archer C50(US)	CVE-2023-30383	Отказ в обслуживании. Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	2023-07-18	https://nvd.nist.gov/vuln/detail/CVE-2023-30383	Есть
	Выполнение произвольного кода в Chrome OS	CVE-2023-4076	Выполнение произвольного кода. Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	2023-08-22	http://chromereleases.googleblog.com/2023/08/long-term-support-channel-update-for_21. • https://bdu.fstec.ru/vul/2023-04492	Есть
	Выполнение произвольного кода в WinRAR	CVE-2023-40477	Выполнение произвольного кода. Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.	2023-08-19	http://www.zerodayinitiative.com/advisories/ZDI-23-1152/ • http://www.win-rar.com/singlenewsview.html?&L=0&tx_ttnews%5Btt_news%5D=232&cHash=	Есть
	Выполнение произвольного кода в Notepad++	CVE-2023-40031	Выполнение произвольного кода. Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.	2023-08-25	https://nvd.nist.gov/vuln/detail/CVE-2023-40031	Есть