ПромСвязьИнвест
расчетная небанковская кредитная организация
367000 РФ, Республика Дагестан, г. Махачкала, ул. Ирчи-Казака 2 «б»
ОКПО 43340114 БИК № 048209395 корсчет 30103810982090000039 5
тел.(8722) 62-16-24, 61-58-22 факс.(8722) 62-16-94 www.psib.ru E-mail: office@psib.ru

«04» марта 2024 г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за февраль 2024 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 февраль 2024 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
1.	Выполнение произвольного кода в Microsoft Edge	CVE-2024-1077	Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы. Последствия эксплуатации: выполнение произвольного кода Рекомендации по устранению: 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.	2024-02-02	http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-1077	Есть
2.	Выполнение произвольного кода в Microsoft Edge	CVE-2024-21399	Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы. Последствия эксплуатации: выполнение произвольного кода Рекомендации по устранению: 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.	2024-02-02	http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21399	Есть
3.	Выполнение произвольного кода в Google Chrome	CVE-2024-1283	Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла. Последствия эксплуатации:	2024-02-07	http://chromereleases.googleblog.com/2024/02/stable-channel-update-for-desktop.html http://crbug.com/41494860	Есть

			выполнение произвольного кода Рекомендации по устранению: 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.			
4.	Отказ в обслуживании в D-Link DIR-815	CVE-2024-22651	Способ эксплуатации: Отправка специально сформированного запроса. Последствия эксплуатации: отказ в обслуживании Рекомендации по устранению: 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.	2024-01-24	нет	Есть
5.	Отказ в обслуживании в Tenda W9	CVE-2024-0541	Способ эксплуатации: Отправка специально сформированного запроса. Последствия эксплуатации: отказ в обслуживании	2024-01-15	https://bdu.fstec.ru/vul/2024-00936	Есть
6.	Выполнение произвольного кода в Microsoft Outlook	CVE-2024-21413	Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки. Последствия эксплуатации: выполнение произвольного кода Рекомендации по устранению: 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.	2024-02-13	http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21413 https://bdu.fstec.ru/vul/2024-01322	Есть
7.	Выполнение произвольного кода в Adobe Acrobat and	CVE-2024-20730	Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла. Последствия эксплуатации:	2024-02-13	http://helpx.adobe.com/security/products/acrobat/apsb24-07.html	Есть

	Reader		выполнение произвольного кода Рекомендации по устранению: 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.			
8.	Выполнение произвольного кода в Microsoft Office	CVE-2024-20673	Способ эксплуатации: Отправка епециально сформированных данных. Последствия эксплуатации: выполнение произвольного кода Рекомендации по устранению: 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.	2024-02-13	http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20673	Есть