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

«02» ноября 2023г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за октябрь 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 подпись **Абдурахманов К.А.**

Приложение № 1
к информационному письму
«Информирование клиентов системы
дистанционного банковского
обслуживания «iBank2» о мерах
защиты за октябрь 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
1.	Выполнение произвольного кода в MySQL Connectors	CVE-2023-22102	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.	2023-10-17	http://www.oracle.com/security-alerts/cpuoct2023.html?3382	Есть
2.	Выполнение произвольного кода в Microsoft Edge	CVE-2023-5218	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.	2023-10-14	http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-5218 https://bdu.fstec.ru/vul/2023-06604	Есть
3.	Получение конфиденциальной информации в Microsoft Edge	CVE-2023-5476	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.	2023-10-14	http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-5218 https://bdu.fstec.ru/vul/2023-06604	Есть
4.	Выполнение произвольного кода в Windows	CVE-2023-36436	выполнение произвольного кода. Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления	2023-10-10	http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36436	Есть

			программного обеспечения только после оценки всех сопутствующих рисков.			
5.	Выполнение произвольного кода в Windows Server	CVE-2023-36557	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.	2023-10-11	http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36557	Есть
6.	Выполнение произвольного кода в Microsoft SQL Server	CVE-2023-36785	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.	2023-10-10	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-36785	Есть
7.	Выполнение произвольного кода в Adobe Photoshop	CVE-2023-26370	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.	2023-10-10	http://helpx.adobe.com/security/products/photoshop/apsb23-51.html	Есть