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

«05» февраля 2024 г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за январь 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 январь 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.	Обход безопасности в Microsoft NET, .NET Framework, and Visual Studio	CVE-2024-0057	Способ эксплуатации: Отправка специально сформированных данных. Последствия эксплуатации: обход безопасности 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.	2024-01-10	http://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-0057	Есть
2.	Выполнение произвольного кода в Google Chrome	CVE-2024-0333	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.	2024-01-09	http://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_9.html	Есть
3.	Выполнение произвольного кода в Microsoft Office	CVE-2024-20677	Способ эксплуатации: Отправка специально сформированных данных. Последствия эксплуатации: выполнение произвольного кода Рекомендации по	2024-01-09	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-20677	Есть

			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.	Повышение привилегий в Google ChromeOS	CVE-2023-39191	Способ эксплуатации: Не определено Последствия эксплуатации: повышение привилегий 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.	2024-01-09	http://chromereleases.googleblog.com/2024/01/stable-channel-update-for-chromeos.html https://bdu.fstec.ru/vul/2023-08557	Есть
5.	Выполнение произвольного кода в Google Chrome и Microsoft Edge	CVE-2024-0225	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.	2024-01-04	http://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop.html http://crbug.com/1506923 http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-0225	Есть
6.	Отказ в обслуживании в Tenda M3	CVE-2023-51095	Способ эксплуатации: Отправка специально сформированных данных. Последствия эксплуатации: отказ в обслуживании Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.	2023-12-26	-	Есть
7.	Чтение локальных файлов в	CVE-2023-41105	Способ эксплуатации: Отправка специально созданных HTTP-запросов.	2024-01-16	http://www.oracle.com/security-alerts/cpujan2024.html?62416	Есть

	MySQL Workbench		Последствия эксплуатации: чтение локальных файлов 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 Foxit PDF Editor for Windows	CVE-2023-51552	Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла. 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.	2024-01-22	http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+11.2.82024-01-22+00%3A00%3A00 https://bdu.fstec.ru/vul/2023-09052	Есть
9.	Выполнение произвольного кода в Mozilla Firefox and Firefox ESR	CVE-2024-0745	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.	2024-01-23	http://www.mozilla.org/en-US/security/advisories/mfsa2024-01/	Есть
10	Повышение привилегий в Mozilla Thunderbird	CVE-2024-0751	Способ эксплуатации: Не определено Последствия эксплуатации: повышение привилегий Рекомендации по устранению: Данная уязвимость устраняется официальным патчем	2024-01-23	http://www.mozilla.org/en-US/security/advisories/mfsa2024-04/	Есть

			вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.			