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» июня 2024 г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за май 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 май 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-2024-4058	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.	2024-04-29	http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-4058	Есть
2.	Выполнение произвольного кода в D-Link routers	CVE-2024-3272	Способ эксплуатации: Использование жестко закодированных учетных данных Последствия эксплуатации: Выполнение произвольного кода Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.	2024-04-08	http://vuldb.com/?id.259283 http://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383 https://bdu.fstec.ru/vul/2024-03256	Есть

3.	Выполнение произвольного кода в Apple iTunes	CVE-2024-27793	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.	2024-05-08	http://support.apple.com/en-us/HT214099	Есть
4.	Выполнение произвольного кода в Google Chrome	CVE-2024-4671	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	2024-05-10	http://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_9.html http://crbug.com/339266700	Есть
5.	Выполнение произвольного кода в Mozilla Firefox	CVE-2024-4768	Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы. Последствия эксплуатации: Выполнение произвольного кода Рекомендации по устранению: Данная	2024-05-15	http://www.mozilla.org/en-US/security/advisories/mfsa2024-21/ http://www.mozilla.org/en-US/security/advisories/mfsa2024-22/	Есть

			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			
6.	Выполнение произвольного кода в Adobe Acrobat и Reader	CVE-2024-34100	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.	2024-05-15	http://helpx.adobe.com/security/products/acrobat/apsb24-29.html	Есть
7.	Получение конфиденциальной информации в LibreOffice	CVE-2024-3044	Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла. Последствия эксплуатации: • Получение конфиденциальной информации Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора.	2024-05-15	http://www.libreoffice.org/about-us/security/advisories/CVE-2024-3044	Есть