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

«16» января 2024 г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за декабрь 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 декабрь 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 Apple macOS Sonoma и Apple Safari	CVE-2023-42917	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.	2023-12-01	http://support.apple.com/en-us/HT214033 http://support.apple.com/en-us/HT214032	Есть
2.	Выполнение произвольного кода в My Calendar плагин WordPress	CVE-2023-6360	Способ эксплуатации: Отправка специально созданных запросов. 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.	2023-11-30	http://www.tenable.com/security/research/tra-2023-40 http://www.joedolson.com/2023/11/my-calendar-3-4-22-security-release/	Есть
3.	Выполнение произвольного кода в Zyxel NAS products	CVE-2023-4474	Способ эксплуатации: Отправка специально сформированных данных. Последствия эксплуатации: выполнение произвольного кода Рекомендации по устранению: Данная уязвимость устраняется официальным патчем	2023-11-30	http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-authentication-bypass-and-command-injection-vulnerabilities-in-nas-products	Есть

			вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.			
4.	Выполнение произвольного кода в Windows	CVE-2023-36006	Способ эксплуатации: Отправка специально 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.	2023-12-12	http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36006	Есть
5.	Выполнение произвольного кода в Adobe After Effects	CVE-2023-48634	Способ эксплуатации: Отправка специально 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.	2023-12-12	http://helpx.adobe.com/security/products/after_effects/apsb23-75.html	Есть
6.	Выполнение произвольного кода в Adobe Illustrator	CVE-2023-47063	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	2023-12-12	http://helpx.adobe.com/security/products/illustrator/apsb23-68.html	Есть

			устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.			
7.	Выполнение произвольного кода в Chrome OS	CVE-2023-5996	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.	2023-12-11	http://chromereleases.googleblog.com/2023/12/long-term-support-channel-update-for.html https://bdu.fstec.ru/vul/2023-07841	Есть
8.	Выполнение произвольного кода в macOS Sonoma	CVE-2023-42899	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.	2023-12-11	https://support.apple.com/en-us/HT214036 https://support.apple.com/en-us/HT214037 https://support.apple.com/en-us/HT214038	Есть
9.	Выполнение произвольного кода в WordPress	None	Способ эксплуатации: Отправка специально созданных запросов. 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.	2023-12-08	http://wordpress.org/documentation/wordpress-version/version-6-4-2/	Есть

10	Выполнение произвольного кода в Microsoft Edge	CVE-2023-6704	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.	2023-12-15	http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-6704 https://bdu.fstec.ru/vul/2023-08754	Есть
11	Выполнение произвольного кода в Google Chrome и Microsoft Edge	CVE-2024-0223	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.	2024-01-04	http://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop.html http://crbug.com/1505009 http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-0223	Есть