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» апреля 2023г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за март 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) 67-72-75, 8(8722) 62-16-94 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 март 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.	Отказ в обслуживании в Microsoft Edge	CVE-2023-0933	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.	2023-02-26	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-0931 http://crbug.com/1407701 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-0929 http://crbug.com/1309035 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-0933 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-0928 http://crbug.com/1399742 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-0927 http://crbug.com/1410766 http://crbug.com/1404864 http://chromereleases.googleblog.com/2023/02/stable-channel-desktop-update_22.html	есть
2.	Выполнение произвольного кода в http	CVE-2023-0941	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.	2023-02-26	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-0931 http://crbug.com/1407701 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-0929 http://crbug.com/1309035 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-0933 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-0928 http://crbug.com/1399742 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-0927 http://crbug.com/1410766 http://crbug.com/1404864 http://chromereleases.googleblog.com/2023/02/stable-channel-desktop-update_22.html http://crbug.com/1414738 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-0930 http://crbug.com/1413005 http://crbug.com/1415366 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-0941 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-0932	есть
3.	Выполнение произвольного кода в Chrome OS	CVE-2022-45934	Последствия эксплуатации: Выполнение произвольного кода Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся	2023-03-05	http://chromereleases.googleblog.com/2023/03/long-term-support-channel-update-for.html https://bdu.fstec.ru/vul/2022-07218	есть

			обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков			
4.	Выполнение произвольного кода в Adobe Illustrator	CVE-2023-26426	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.	2023-03-14	http://helpx.adobe.com/security/products/illustrator/apsb23-19.html	есть
5.	Получение конфиденциальной информации в Microsoft Outlook	CVE-2023-23397	Последствия эксплуатации: Получение конфиденциальной информации 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.	2023-03-14	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-23397	есть
6.	Выполнение произвольного кода в Mozilla Thunderbird	CVE-2023-28176	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.	2023-03-15	http://www.mozilla.org/en-US/security/advisories/mfsa2023-11/	есть
7.	Выполнение произвольного кода в Windows	CVE-2023-23404	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.	2023-03-14	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-23404	есть
8.	Выполнение произвольного кода в Windows	CVE-2023-23401	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.	2023-03-14	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-23401	есть
9.	Выполнение произвольного кода в http	CVE-2023-23405	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	2023-03-14	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-23405	есть

			обеспечения только после оценки всех сопутствующих рисков.			
10.	Выполнение произвольного кода в Microsoft Edge	CVE-2023-1222	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.	2023-03-14	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-1222 https://bdu.fstec.ru/vul/2023-01243	есть
11.	Выполнение произвольного кода в Microsoft Edge	CVE-2023-1213	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.	2023-03-14	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-1213	есть