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

«05» июня 2023г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за май 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 май 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.	Чтение локальных файлов в Ubuntu	CVE-2023-28756	Способ эксплуатации: Отправка специально созданных HTTP-запросов. 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.	2023-05-04	http://ubuntu.com/security/notices/USN-6055-1 https://bdu.fstec.ru/vul/2023-02020	есть
2.	Получение конфиденциальной информации в Gentoo Linux	CVE-2022-46882	Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы. 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.	2023-05-03	http://security.gentoo.org/glsa/202305-13	есть
3.	Отказ в обслуживании в OpenSSL	CVE-2023-0464	Способ эксплуатации: Отправка специально сформированных данных. 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.	2023-05-10	http://www.ibm.com/support/pages/node/6989163 https://bdu.fstec.ru/vul/2023-02108 https://www.openssl.org/news/secadv/20230322.txt http://repo.red-soft.ru/redos/7.3c/x86_64/updates/ https://www.suse.com/security/cve/CVE-2023-0464.html https://access.redhat.com/security/cve/CVE-2023-0464 https://security-tracker.debian.org/tracker/CVE-2023-0464 https://nvd.nist.gov/vuln/detail/CVE-2023-0464	есть
4.	Получение конфиденциальной информации в Chrome OS	CVE-2023-2461	Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы. 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.	2023-05-10	http://chromereleases.googleblog.com/2023/05/stable-channel-update-for-chromeos.html	есть
5.	Выполнение произвольного кода в Windows	CVE-2023-24903	Способ эксплуатации: Не определено. Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только	2023-05-09	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-24903	есть

			после оценки всех сопутствующих рисков.			
6.	Отказ в обслуживании в Windows	CVE-2023-24940	Способ эксплуатации: Отправка специально сформированных данных. 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.	2023-05-09	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-24940	есть
7.	Выполнение произвольного кода в Microsoft Office	CVE-2023-24953	Способ эксплуатации: Отправка специально сформированных данных. 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.	2023-05-09	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-24953	есть
8.	Межсайтовый скриптинг в Mozilla Firefox	CVE-2023-32207	Способ эксплуатации: Не определено. 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.	2023-05-09	http://www.mozilla.org/en-US/security/advisories/mfsa2023-16/ http://www.mozilla.org/en-US/security/advisories/mfsa2023-17/	есть
9.	Отказ в обслуживании в Mozilla Firefox	CVE-2023-32206	Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы. 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.	2023-05-09	http://www.mozilla.org/en-US/security/advisories/mfsa2023-16/ http://www.mozilla.org/en-US/security/advisories/mfsa2023-17/	есть
10.	Выполнение произвольного кода в Microsoft Edge	CVE-2023-29350	Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы. 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.	2023-05-06	http://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-29350	есть
11.	Выполнение произвольного кода в MikroTik RouterOS	CVE-2023-32154	Способ эксплуатации: Отправка специально сформированных данных. 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.	2023-05-18	https://www.zerodayinitiative.com/advisories/ZDI-23-710/ https://bdu.fstec.ru/vul/2023-02827	есть