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

«03» мая 2023г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за апрель 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 апрель 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 Ubuntu	CVE-2023-24538	Выполнение произвольного кода. 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.	2023-04-25	http://www.suse.com/support/update/announcement/2023/suse-su-20231979-1/	есть
	Отказ в обслуживании в Ubuntu	CVE-2022-2879	Отправка специально созданного вредоносного файла. 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.	2023-04-25	http://ubuntu.com/security/notices/USN-6038-1	есть
	Повышение привилегий в Git for Windows	CVE-2023-29011	Открытие пользователем специально созданного вредоносного файла. 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.	2023-04-25	http://github.com/git-for-windows/git/releases/tag/v2.40.1.windows.1 • http://github.com/git-for-windows/git/security/advisories/GHSA-g4fv-xjqw-q7jm	есть
	Выполнение произвольного кода в VMware Workstation	CVE-2023-20872	Выполнение произвольного кода. 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.	2023-04-25	http://www.vmware.com/security/advisories/VMSA-2023-0008.html	есть
	Получение конфиденциальной информации в Oracle Linux	CVE-2023-25725	Отправка специально созданных HTTP-запросов. Получение конфиденциальной информации. 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.	2023-04-24	http://www.oracle.com/security-alerts/linuxbulletinapr2023.html • https://bdu.fstec.ru/vul/2023-00758	есть

	Выполнение произвольного кода в Red Hat Enterprise Linux for ARM 64	CVE-2023-28205	Открытие пользователем специально созданной вредоносной веб-страницы.Выполнение произвольного кода. 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.	2023-04-21	http://access.redhat.com/errata/RHSA-2023:1918	есть
	Выполнение произвольного кода в Linux	CVE-2023-28772	Выполнение произвольного кода.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.	2023-03-23	https://nvd.nist.gov/vuln/detail/CVE-2023-28772 • https://github.com/torvalds/linux/commit/d3b16034a24a112bb83acb669ac5b9b01f744bb7 • https://lore.kernel.org/lkml/20210625122453.5e2fe304@oasis.local.home/	есть
	Повышение привилегий в Debian GNU/Linux, Linux	CVE-2023-0386	Обход процесса авторизации. Повышение привилегий. 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.	2023-03-22	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=4f11ada10d0a • https://mirrors.edge.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.15.91 • https://mirrors.edge.kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.1.9 • https://security-tracker.debian.org/tracker/CVE-2023-0386 • https://bdu.fstec.ru/vul/2023-01572	есть