ПромСвязьИнвест
расчетная небанковская кредитная организация
367000 РФ, Республика Дагестан, г. Махачкала, ул. Ирчи-Казака 2 «б»
ОКПО 43340114 БИК № 048209395 корсчет 30103810982090000395
тел.(8722) 62-16-24, 61-58-22 факс.(8722) 62-16-94 www.psib.ru E-mail: office@psib.ru

«01» февраля 2022г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за январь 2022 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.

Председатель Правления _____ **Абдурахманов К.А.**
подпись

Приложение № 1
к информационному письму
«Информирование клиентов системы
дистанционного банковского
обслуживания «iBank2» о мерах
защиты за январь 2022 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	Повышение привилегий в Linux kernel	MITRE: CVE-2022-0185	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе посредством специально созданной вредоносного кода. Уязвимость обусловлена целочисленным переполнением.	18 января 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022011820 http://github.com/torvalds/linux/commit/3e1aeb00e6d132efc151dacc062b38269bc9eccc#diff-c4a9ea83de4a42a0d1bcbaf1f03ce35188f38da4987e0e7a52aae7f04de14a05 http://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=722d94847de29310e8aa03fcbdb41fc92c521756	Есть
	Множественные уязвимости в Apple iOS	MITRE: CVE-2022-22584	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.	26 января 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022012633 http://support.apple.com/en-us/HT213056 http://support.apple.com/en-us/HT213053	
	Выполнение произвольного кода в Apple Safari	MITRE: CVE-2022-22590	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой использования после освобождения.	26 января 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022012702 http://support.apple.com/en-us/HT213053	
	Повышение привилегий в polkit pkexec	MITRE: CVE-2021-4034	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе посредством создания специально сформированных переменных для pkexec. Уязвимость обусловлена некорректной проверкой входных данных.	26 января 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022012601 http://gitlab.freedesktop.org/polkit/polkit/-/commit/a2bf5c9c83b6ae46cbd5c779d3055bff81ded683 http://bugzilla.redhat.com/show_bug.cgi?id=2025869	
	Выполнение произвольного кода в Foxit PDF Reader и Editor for Mac	Не определен	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного PDF-файла. Уязвимость обусловлена граничным условием.	25 января 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022012505 http://www.foxitsoftware.com/support/security-bulletins.html	
	Множественные уязвимости в ПО IBM	MITRE: CVE-2021-45105	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных данных. Уязвимость обусловлена	24 января 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022012438 https://www.cybersecurity-help.cz/vdb/SB2022012440 https://www.cybersecurity-help.cz/vdb/SB2022012441 https://www.cybersecurity-	

			зацикливанием внутри класса. 24 января 2022 г.		help.cz/vdb/SB2022012442 https://www.cybersecurity-help.cz/vdb/SB2022012443 http://www.ibm.com/blogs/psirt/security-bulletin-ibm-disconnected-log-collector-is-vulnerable-to-denial-of-service-and-arbitrary-code-execution-due-to-apache-log4j-cve-2021-45105-and-cve-2021-45046/ http://www.ibm.com/support/pages/node/6541922 http://www.ibm.com/blogs/psirt/security-bulletin-ibm-integrated-analytics-system-is-vulnerable-to-denial-of-service-and-arbitrary-code-execution-due-to-apache-log4j-cve-2021-45105-cve-2021-45046/ http://www.ibm.com/support/pages/node/6541930 http://www.ibm.com/blogs/psirt/security-bulletin-due-to-the-use-of-apache-log4j-ibm-spectrum-symphony-is-vulnerable-to-arbitrary-code-execution-cve-2021-44832-and-cve-2021-45046-and-denial-of-service-cve-2021-45105/ http://www.ibm.com/support/pages/node/6539410 http://www.ibm.com/blogs/psirt/security-bulletin-due-to-the-use-of-apache-log4j-ibm-spectrum-conductor-is-vulnerable-to-arbitrary-code-execution-cve-2021-44832-and-cve-2021-45046-and-denial-of-service-cve-2021-45105/ http://www.ibm.com/support/pages/node/6541736 http://www.ibm.com/blogs/psirt/security-bulletin-ibm-operations-analytics-predictive-insights-is-vulnerable-to-denial-of-service-and-arbitrary-code-execution-due-to-apache-log4j-cve-2021-45105-cve-2021-45046/ http://www.ibm.com/support/pages/node/6549360	
	Множественные уязвимости в Oracle VM Server	MITRE: CVE-2017-17045	Эксплуатация уязвимости позволяет удаленному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена некорректными ограничениями безопасности.	19 января 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022011910 http://www.oracle.com/security-alerts/ovmbulletinjan2022.html	
	Выполнение произвольного кода в ПО Oracle	MITRE: CVE-2021-2351	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных.	19 января 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022011824 https://www.cybersecurity-help.cz/vdb/SB2022011825 https://www.cybersecurity-help.cz/vdb/SB2022011826 https://www.cybersecurity-help.cz/vdb/SB2022011832 https://www.cybersecurity-help.cz/vdb/SB2022011833 https://www.cybersecurity-help.cz/vdb/SB2022011834 http://www.oracle.com/security-alerts/cpujul2021.html http://www.oracle.com/security-alerts/cpujan2022.html?61750 http://www.oracle.com/security-alerts/cpujan2022.html http://www.oracle.com/security-alerts/cpujan2022.html?947510 http://www.oracle.com/security-alerts/cpujan2022.html?924165 http://www.oracle.com/security-alerts/cpujan2022.html?3354	
	Множественные уязвимости в Google Chrome	MITRE: CVE-2022-0290 CVE-2022-0293 CVE-2022-0295 CVE-2022-0296 CVE-2022-0297 CVE-2022-0298 CVE-2022-	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой использования после освобождения.	19 января 2022 г.	http://crbug.com/1270358 http://crbug.com/1278613 http://crbug.com/1284367 http://crbug.com/1281979 http://crbug.com/1283375 http://crbug.com/1276331 http://crbug.com/1275438 http://crbug.com/1282118 http://crbug.com/1278180 http://crbug.com/1283805 http://crbug.com/1283371	

		0300 CVE-2022-0302 CVE-2022-0304			http://crbug.com/1282354 http://crbug.com/1273017 http://crbug.com/1260007 http://crbug.com/1212957	
	Выполнение произвольного кода в Apache Log4j	MITRE: CVE-2022-23302	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных при обработке сериализованных данных.	18 января 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022011818 http://lists.apache.org/thread/bsr3l5qz4g0myrjhy9h67bcxodpkwj4w http://logging.apache.org/log4j/1.2/index.html	
	Запросы к произвольным системам в Oracle HTTP Server	MITRE: CVE-2021-40438	Эксплуатация уязвимости позволяет удаленному злоумышленнику инициализировать запросы к произвольным системам с уязвимого веб-сервера посредством отправки специально сформированного HTTP-пакета. Уязвимость обусловлена некорректной проверкой введенных данных.	18 января 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022011836 http://www.oracle.com/security-alerts/cpujan2022.html?1389	