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» мая 2022г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за апрель 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 апрель 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.	Выполнение произвольного кода в Jira	MITRE: CVE-2022-0540	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного HTTP-запроса. загрузки. Уязвимость обусловлена некорректной работой процесса аутентификации.	20 апреля 2022 г.	http://confluence.atlassian.com/display/JIRA/Jira+Security+Advisory+2022-04-20 http://jira.atlassian.com/browse/JSDSERVER-11224 http://jira.atlassian.com/browse/JRASERVER-73650	Есть
2.	Выполнение произвольных команд в D-Link DIR-878	MITRE: CVE-2022-26670	Эксплуатация уязвимости позволяет злоумышленнику из смежной сети выполнить произвольные команды в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных.	07 апреля 2022 г.	https://www.twcert.org.tw/tw/cp-132-5972-c259e-1.html	Есть
3.	Выполнение произвольного кода в Microsoft Remote Procedure Call Runtime	MITRE: CVE-2022-26809	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специального сформированного RPC-вызова. Уязвимость обусловлена некорректной проверкой входных данных.	12 апреля 2022 г.	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26809	Есть
4.	Множественные уязвимости в Google ChromeOS	MITRE: CVE-2022-1131	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. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-416: Использование после освобождения 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.	15 апреля 2022 г.	http://chromereleases.googleblog.com/2022/04/long-term-support-channel-update_15.html	Есть
5.	Множественные уязвимости в Google Chrome	MITRE: CVE-2022-1305 CVE-2022-1308 CVE-2022-1310 CVE-	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально	11 апреля 2022 г.	http://chromereleases.googleblog.com/2022/04/stable-channel-update-for-desktop_11.html	Есть

		2022-1311 CVE-2022-1312	созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой использования после освобождения. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-416: Использование после освобождения 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.			
6.	Выполнение произвольного кода в Google Chrome	MITRE: CVE-2022-1364	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой смешения типов.	15 апреля 2022 г.	http://chromereleases.googleblog.com/2022/04/stable-channel-update-for-desktop_14.html http://crbug.com/1315901	Есть
7.	Выполнение произвольного кода в Adobe After Effects	MITRE: CVE-2022-27783 CVE-2022-27784	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.	12 апреля 2022 г.	http://helpx.adobe.com/security/products/after_effects/apsb22-19.html	Есть
8.	Выполнение произвольного кода в 7-Zip	MITRE: CVE-2022-29072	Эксплуатация уязвимости позволяет злоумышленнику выполнить произвольный код в целевой системе с правами администратора. Уязвимость обусловлена ошибкой границ памяти.	18 апреля 2022 г.	http://sourceforge.net/p/sevenzip/bugs/2337/ http://www.youtube.com/watch?v=sT1cvbu7ZTA http://github.com/kagancapar/CVE-2022-29072 http://news.ycombinator.com/item?id=31070256	Есть
9.	Выполнение произвольного кода в Microsoft Edge	MITRE: CVE-2022-29144	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной проверкой входных данных.	15 апреля 2022 г.	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29144	Есть
10.	Загрузка вредоносного файла в TYPO3	Не определен	Эксплуатация уязвимости позволяет удаленному злоумышленнику загрузить и выполнить вредоносный файл на уязвимом сервере. Уязвимость обусловлена некорректной проверкой файла во время загрузки.	26 апреля 2022 г.	http://typo3.org/security/advisory/typo3-ext-sa-2022-005/	Есть
11.	Выполнение произвольного кода в Apple iOS, iPadOS и Apple macOS Monterey	MITRE: CVE-2022-22675	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством запуска специально созданной вредоносной программы. Уязвимость обусловлена ошибкой границ памяти.	01 апреля 2022 г.	http://support.apple.com/en-us/HT213219 http://support.apple.com/en-us/HT213220	Есть
12.	Выполнение произвольного кода в Spring Framework	MITRE: CVE-2022-22965	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки	31 марта 2022 г.	http://lab.wallarm.com/update-on-0-day-vulnerabilities-in-spring-spring4shell-and-cve-2022-22963/ http://tanzu.vmware.com/security/cve-2022-22965 http://spring.io/blog/2022/03/31/spring-	Есть

			специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных		framework-rce-early-announcement	
13.	Удаленное выполнение кода в IP-камерах TP-Link Tapo	MITRE: CVE-2021-4045	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных в файле uhttpd.	10 марта 2022 г.	https://www.incibe-cert.es/en/early-warning/security-advisories/tp-link-tapo-c200-remote-code-execution-vulnerability https://nvd.nist.gov/vuln/detail/CVE-2021-4045	Есть
14.	Множественные уязвимости в Mozilla Firefox	MITRE: CVE-2022-1097 CVE-2022-1196 CVE-2022-28282	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.	05 апреля 2022 г.	http://www.mozilla.org/en-US/security/advisories/mfsa2022-13/ http://www.mozilla.org/en-US/security/advisories/mfsa2022-14/	Есть
15.	Множественные уязвимости в Mozilla Thunderbird	MITRE: CVE-2022-1097 CVE-2022-1196 CVE-2022-28282	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специального созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой использования после освобождения.	06 апреля 2022 г.	http://www.mozilla.org/en-US/security/advisories/mfsa2022-15/	Есть
16.	Выполнение произвольного кода в Microsoft Edge	MITRE: CVE-2022-1232	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной проверкой входных данных.	07 апреля 2022 г.	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-1232	Есть
17.	Выполнение произвольных SQL-запросов в Django	MITRE: CVE-2022-28346 CVE-2022-28347	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные SQL-запросы к базе данных уязвимого приложения посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных.	11 апреля 2022 г.	http://www.djangoproject.com/weblog/2022/apr/11/security-releases/	Есть