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

«01» августа 2022г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за июль 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 июль 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.	Множественные уязвимости в Microsoft Edge	MITRE: CVE-2022-2477 CVE-2022-2478 CVE-2022-2480 CVE-2022-2481	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.	23 июля 2022 г.	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-2479 http://crbug.com/1335861 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-2478 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-2481 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-2477 http://chromereleases.googleblog.com/2022/07/stable-channel-update-for-desktop_19.html http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-2480 http://crbug.com/1341603 http://crbug.com/1336266 http://crbug.com/1339844 http://crbug.com/1329987	Есть
2.	Множественные уязвимости в Google Chrome	MITRE: CVE-2022-2477 CVE-2022-2478 CVE-2022-2480 CVE-2022-2481	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 июля 2022 г.	http://chromereleases.googleblog.com/2022/07/stable-channel-update-for-desktop_19.html http://crbug.com/1341603 http://crbug.com/1329987 http://crbug.com/1339844 http://crbug.com/1336266 http://crbug.com/1335861	Есть
3.	Множественные уязвимости в Google Chrome	MITRE: CVE-2022-2479	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.	19 июля 2022 г.	http://chromereleases.googleblog.com/2022/07/stable-channel-update-for-desktop_19.html http://crbug.com/1341603 http://crbug.com/1329987 http://crbug.com/1339844 http://crbug.com/1336266 http://crbug.com/1335861	Есть
4.	Выполнение произвольного кода в Mozilla Firefox и Firefox ESR	MITRE: CVE-2022-2505 CVE-2022-36320	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти.	26 июля 2022 г.	http://www.mozilla.org/en-US/security/advisories/mfsa2022-28/ http://www.mozilla.org/en-US/security/advisories/mfsa2022-30/	Есть
5.	Множественные уязвимости в Chrome OS	MITRE: CVE-2022-2156	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой использования после освобождения.	18 июля 2022 г.	http://chromereleases.googleblog.com/2022/07/long-term-support-channel-update-for.html	Есть

6.	Множественные уязвимости в Chrome OS	MITRE: CVE-2021-30560	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.	18 июля 2022 г.	http://chromereleases.googleblog.com/2022/07/long-term-support-channel-update-for.html	Есть
7.	Множественные уязвимости в Chrome OS	MITRE: CVE-2022-29824	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена целочисленным переполнением.	18 июля 2022 г.	http://chromereleases.googleblog.com/2022/07/long-term-support-channel-update-for.html	Есть
8.	Выполнение произвольных команд ОС в продуктах Zyxel	MITRE: CVE-2022-30526	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольные команды ОС с привилегиями «root» в целевой системе. Уязвимость обусловлена некорректными ограничениями безопасности.	19 июля 2022 г.	http://www.zyxel.com/support/Zyxel-security-advisory-authenticated-directory-traversal-vulnerabilities-of-firewalls.shtml	Есть
9.	Выполнение произвольного кода в PHP	MITRE: CVE-2022-31627	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена ошибкой границ памяти.	14 июля 2022 г.	http://bugs.php.net/bug.php?id=81723 http://www.php.net/ChangeLog-8.php#8.1.8	Есть
10.	Выполнение произвольного кода в Foxit PDF Reader and Editor	MITRE: Не определен	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного PDF-файла. Уязвимость обусловлена ошибкой использования после освобождения.	28 июня 2022 г.	http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Reader+12.0+and+Foxit+PDF+Editor+12.01970-01-01+01%3A00%3A00	Есть