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

«06» сентября 2021г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за август 2021 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

М.П.

Исп. Ирганов Ю.Г.:
руководитель СИБ
8 (8722) 67-72-75

Приложение № 1
к информационному письму
«Информирование клиентов системы
дистанционного банковского
обслуживания «iBank2» о мерах
защиты за август 2021 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 OpenSSL	MITRE: CVE-2021-3711	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена ошибкой границ памяти в функции EVP_PKEY_decrypt() в реализации дешифрования SM2.	24 августа 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021082414 https://www.openssl.org/news/secadv/20210824.txt https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=59f5e75f3bced8fc0e130d72a3f582cf7b480b46	Есть
2.	Выполнение произвольного кода в BlackBerry QNX SDP и QNX OS	MITRE: CVE-2021-22156	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена целочисленным переполнением в функции calloc() в библиотеке среды выполнения C.	18 августа 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021082304 https://support.blackberry.com/kb/articleDetail?articleNumber=000082334 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-qnx-TOxjVPdL	Есть
3.	Выполнение произвольного кода в маршрутизаторах Cisco	MITRE: CVE-2021-34730	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных UPnP-запросов. Уязвимость обусловлена ошибкой границ памяти в службе Universal Plug-and-Play (UPnP).	18 августа 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021082201 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cisco-sb-rv-overflow-htpymMB5 https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvz05607	нет
4.	Множественные уязвимости в Realtek SDK	MITRE: CVE-2021-35392	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных запросов. Уязвимость обусловлена некорректным созданием сообщений SSDP NOTIFY из заголовка ST, полученных сообщений M-SEARCH.	17 августа 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021081709 https://www.iot-inspector.com/blog/advisory-multiple-issues-realtek-sdk-iot-supply-chain https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2021-35392_35395.pdf https://www.realtek.com/en/cu-1-en/cu-1-taiwan-en	Есть
5.	Множественные уязвимости в Realtek SDK	MITRE: CVE-2021-35394	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды оболочки в целевой системе посредством отправки специально сформированных данных в уязвимое приложение. Уязвимость обусловлена некорректной проверкой входных данных в диагностическом инструменте MP Daemon.	17 августа 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021081709 https://www.iot-inspector.com/blog/advisory-multiple-issues-realtek-sdk-iot-supply-chain https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2021-35392_35395.pdf https://www.realtek.com/en/cu-1-en/cu-1-taiwan-en	Есть
6.	Множественные уязвимости в	MITRE: CVE-2021-35393	Эксплуатация уязвимости позволяет удаленному	17 августа 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021081709 https://www.iot-	Есть

	Realtek SDK		злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректным синтаксическим анализом заголовка обратного вызова UPnP SUBSCRIBE / UNSUBSCRIBE.		inspector.com/blog/advisory-multiple-issues-realtek-sdk-iot-supply-chain https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2021-35392_35395.pdf https://www.realtek.com/en/cu-1-en/cu-1-taiwan-en	
7.	Множественные уязвимости в Adobe Photoshop	MITRE: CVE-2021-36065	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного файла. Уязвимость обусловлена ошибкой границ памяти.	18 августа 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021081806 https://helpx.adobe.com/security/products/photoshop/apsb21-68.html	Есть
8.	Множественные уязвимости в Adobe Photoshop	MITRE: CVE-2021-36066	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного файла. Уязвимость обусловлена ошибкой границ памяти.	18 августа 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021081806 https://helpx.adobe.com/security/products/photoshop/apsb21-68.html	Есть
9.	Множественные уязвимости в Google Chrome	MITRE: CVE-2021-30598 CVE-2021-30599	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой смешения типов.	17 августа 2021 г.	https://bugs.chromium.org/p/chromium/issues/detail?id=1234764 https://bugs.chromium.org/p/chromium/issues/detail?id=1234770 https://bugs.chromium.org/p/chromium/issues/detail?id=1234009 https://bugs.chromium.org/p/chromium/issues/detail?id=1233564 https://bugs.chromium.org/p/chromium/issues/detail?id=1230767 https://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop.html https://www.cybersecurity-help.cz/vdb/SB2021081702 https://bugs.chromium.org/p/chromium/issues/detail?id=1234829 https://bugs.chromium.org/p/chromium/issues/detail?id=1231134	Есть
10.	Множественные уязвимости в Google Chrome	MITRE: CVE-2021-30600 CVE-2021-30601 CVE-2021-30602	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.	17 августа 2021 г.	https://bugs.chromium.org/p/chromium/issues/detail?id=1234764 https://bugs.chromium.org/p/chromium/issues/detail?id=1234770 https://bugs.chromium.org/p/chromium/issues/detail?id=1234009 https://bugs.chromium.org/p/chromium/issues/detail?id=1233564 https://bugs.chromium.org/p/chromium/issues/detail?id=1230767 https://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop.html https://www.cybersecurity-help.cz/vdb/SB2021081702 https://bugs.chromium.org/p/chromium/issues/detail?id=1234829 https://bugs.chromium.org/p/chromium/issues/detail?id=1231134	Есть
11.	Множественные уязвимости в Google Chrome	MITRE: CVE-2021-30603	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена состоянием гонки в WebAudio.	17 августа 2021 г.	https://bugs.chromium.org/p/chromium/issues/detail?id=1234764 https://bugs.chromium.org/p/chromium/issues/detail?id=1234770 https://bugs.chromium.org/p/chromium/issues/detail?id=1234009 https://bugs.chromium.org/p/chromium/issues/detail?id=1233564 https://bugs.chromium.org/p/chromium/issues/detail?id=1230767 https://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop.html https://www.cybersecurity-help.cz/vdb/SB2021081702 https://bugs.chromium.org/p/chromium/issues	Есть

					/detail?id=1234829 https://bugs.chromium.org/p/chromium/issues/detail?id=1231134	
12.	Множественные уязвимости в Google Chrome	MITRE: CVE-2021-30604	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.	17 августа 2021 г.	https://bugs.chromium.org/p/chromium/issues/detail?id=1234764 https://bugs.chromium.org/p/chromium/issues/detail?id=1234770 https://bugs.chromium.org/p/chromium/issues/detail?id=1234009 https://bugs.chromium.org/p/chromium/issues/detail?id=1233564 https://bugs.chromium.org/p/chromium/issues/detail?id=1230767 https://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop.html https://www.cybersecurity-help.cz/vdb/SB2021081702 https://bugs.chromium.org/p/chromium/issues/detail?id=1234829 https://bugs.chromium.org/p/chromium/issues/detail?id=1231134	Есть
13.	Выполнение произвольного кода в Microsoft Windows Media MPEG-4 Video Decoder	MITRE: CVE-2021-36937	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных в видео декодере Windows Media MPEG-4.	10 августа 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021081032 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36937	Есть
14.	Выполнение произвольного кода в Microsoft Remote Desktop Client и Hyper-V Viewer	MITRE: CVE-2021-34535	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных в клиенте удаленного рабочего стола и средстве просмотра Hyper-V.	10 августа 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021081025 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34535	Есть
15.	Выполнение произвольного кода в Microsoft Office	MITRE: CVE-2021-36941	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных.	10 августа 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021081028 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36941	Есть
16.	Выполнение произвольного кода в Microsoft Office	MITRE: CVE-2021-36941	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных.	10 августа 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021081028 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36941	Есть
17.	Выполнение произвольного кода в Google Chrome	MITRE: CVE-2021-30590	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти при обработке HTML-данных.	2 августа 2021 г.	https://crbug.com/1229298 https://crbug.com/1209469 https://chromereleases.googleblog.com/2021/08/the-stable-channel-has-been-updated-to.html https://crbug.com/1218468 https://www.cybersecurity-help.cz/vdb/SB2021080211 https://crbug.com/1227777	Есть
18.	Выполнение произвольного кода в Google Chrome	MITRE: CVE-2021-30591	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия	2 августа 2021 г.	https://crbug.com/1229298 https://crbug.com/1209469 https://chromereleases.googleblog.com/2021/08/the-stable-channel-has-been-updated-to.html https://crbug.com/1218468	Есть

			пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой использования после освобождения в компоненте API файловой системы в Google Chrome.		https://www.cybersecurity-help.cz/vdb/SB2021080211 https://crbug.com/1227777	
19.	Выполнение произвольного кода в Google Chrome	MITRE: CVE-2021-30592	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти при обработке HTML-данных в группах вкладок.	2 августа 2021 г.	https://crbug.com/1229298 https://crbug.com/1209469 https://chromereleases.googleblog.com/2021/08/the-stable-channel-has-been-updated-to.html https://crbug.com/1218468 https://www.cybersecurity-help.cz/vdb/SB2021080211 https://crbug.com/1227777	Есть
20.	Выполнение произвольного кода в Google Chrome	MITRE: CVE-2021-30594	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 в компоненте пользовательского интерфейса «Информация о странице» в Google Chrome.	2 августа 2021 г.	https://crbug.com/1229298 https://crbug.com/1209469 https://chromereleases.googleblog.com/2021/08/the-stable-channel-has-been-updated-to.html https://crbug.com/1218468 https://www.cybersecurity-help.cz/vdb/SB2021080211 https://crbug.com/1227777	Есть