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

«17» мая 2021г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за апрель 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 _____ **К.А.Абдурахманов**
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 апрель 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.	Множественные уязвимости в Google Chrome Google Chrome: 87.0.4280.66, 87.0.4280.141, 88.0.4324.96, 88.0.4324.146, 88.0.4324.150, 88.0.4324.182, 89.0.4389.72, 89.0.4389.90, 89.0.4389.114, 89.0.4389.128, 90.0.4430.72	MITRE: CVE-2021-21222, MITRE: CVE-2021-21224	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 движке браузера V8.	20 апреля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021042013 https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_20.html	Есть
2.	Выполнение произвольного кода в WebKitGTK	CWE-119: Выполнение операций за пределами буфера памяти CWE-416: Использование после освобождения	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной веб-страницы. Уязвимость обусловлена некорректной обработкой веб-контента.	27 апреля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021042801 https://support.apple.com/en-us/HT212325	Есть
3.	Выполнение произвольного кода в ПО компании Mozilla	MITRE: CVE-2021-23995	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 ненадежных входных данных при включенном режиме адаптивного дизайна.	19 апреля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021041920 https://www.cybersecurity-help.cz/vdb/SB2021041919 https://www.mozilla.org/en-US/security/advisories/mfsa2021-16/ https://www.mozilla.org/en-US/security/advisories/mfsa2021-15/ https://www.mozilla.org/en-US/security/advisories/mfsa2021-14/	Есть
4.	Множественные уязвимости в Oracle VM VirtualBox	MITRE: CVE-2021-2264, MITRE: CVE-2021-2250, MITRE: CVE-2021-2279	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику получить НСД к данным в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных в компоненте Core в Oracle VM VirtualBox.	21 апреля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021042113 https://www.oracle.com/security-alerts/cpuapr2021.html https://www.oracle.com/security-alerts/cpuapr2021verbose.html	Есть
5.	Выполнение произвольных команд в Symantec Security Analytics	MITRE: CVE-2021-30642	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды оболочки с повышением привилегий в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена	20 апреля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021042015 https://support.broadcom.com/security-advisory/security-advisory-detail.html?notificationId=SYMSA17969	Есть

			некорректной проверкой входных данных в веб-интерфейсе Symantec Security Analytics.			
6.	Множественные уязвимости в Oracle Secure Global Desktop	MITRE: CVE-2021-2177 CVE-2021-2248, MITRE: CVE-2021-2221	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных в клиентском компоненте Oracle Secure Global Desktop.	21 апреля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021042114 https://www.oracle.com/security-alerts/cpuapr2021.html https://www.oracle.com/security-alerts/cpuapr2021verbose.html	Есть
7.	Повышение привилегий в Microsoft Windows	MITRE: CVE-2021-28310	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе посредством запуска специально созданной вредоносной программы. Уязвимость обусловлена ошибкой границ буфера памяти в драйвере win32k.sys	13 апреля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021041347 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28310 https://securelist.com/zero-day-vulnerability-in-desktop-window-manager-cve-2021-28310-used-in-the-wild/101898/	Есть
8.	Множественные уязвимости в Microsoft Exchange Server	MITRE: CVE-2021-28480 CVE-2021-28481, MITRE: CVE-2021-28482, MITRE: CVE-2021-28483	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного запроса. Уязвимость обусловлена некорректной проверкой входных данных.	13 апреля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021041327 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28480 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28481 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28482 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28483	Есть
9.	Выполнение произвольного кода в macOS	MITRE: CVE-2021-1788	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной веб-страницы. Уязвимость обусловлена некорректным функционированием компонента WebKit.	2 февраля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021033006 https://support.apple.com/en-us/HT212147	Есть
10.	Выполнение произвольного кода в Apple Safari	MITRE: CVE-2021-1844	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной веб-страницы. Уязвимость обусловлена некорректной обработкой веб-контента компонентом WebKit.	8 марта 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021033006 https://support.apple.com/en-us/HT212223	Есть
11.	Выполнение произвольного кода в Apple iOS	MITRE: CVE-2021-1871	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной веб-страницы. Уязвимость обусловлена некорректным функционированием компонента WebKit.	27 января 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021033006 https://support.apple.com/en-us/HT212146	Есть
12.	Отказ в обслуживании в продуктах компании Huawei	MITRE: CVE-2021-22320	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании в целевой системе посредством отправки вредоносных сообщений. Уязвимость обусловлена некорректной обработкой сообщений.	24 февраля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021022409 https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210210-03-dos-en	Есть
13.	Отказ в обслуживании в продуктах	MITRE: CVE-2021-1352	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в	24 марта 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021032417 https://tools.cisco.com/security/center/content/	Есть

	компании Cisco		обслуживании в целевой системе посредством отправки специально созданного вредоносного DECnet-пакета. Уязвимость обусловлена некорректной проверкой DECnet-пакетов.		CiscoSecurityAdvisory/cisco-sa-iosxe-decnet-dos-cuPWDkyL https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvv51476	