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» апреля 2021г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за март 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 март 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.	Критические уязвимости в Microsoft Exchange Server	CVE-2021-26855	SSRF уязвимость в Exchange, позволяющая злоумышленникам отправлять специальные HTTP запросы для аутентификации на сервере	3 марта 2021 г.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855	Есть
2.	Критические уязвимости в Microsoft Exchange Server	CVE-2021-26412	RCE уязвимость в Exchange, позволяющая злоумышленнику выполнить произвольный код на сервере Exchange	3 марта 2021 г.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26412	Есть
3.	Критические уязвимости в Microsoft Exchange Server	CVE-2021-27078	RCE уязвимость в Exchange, позволяющая злоумышленнику выполнить произвольный код на сервере Exchange	3 марта 2021 г.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-27078	Есть
4.	Критические уязвимости в Microsoft Exchange Server	CVE-2021-26857	Уязвимость небезопасной десериализации в Exchange, позволяющая выполнять на сервере Exchange код от имени пользователя SYSTEM	3 марта 2021 г.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26857	Есть
5.	Выполнение произвольного кода в VMware ESXi	MITRE: CVE-2020-21974	Эксплуатация уязвимости позволяет злоумышленнику, находящемуся в смежной сети, выполнить произвольный код в целевой системе посредством отправки специально сформированных сетевых пакетов на порт 427. Уязвимость обусловлена некорректным функционированием компонента OpenSLP.	23 февраля 2021 г.	https://www.vmware.com/security/advisories/VMSA-2021-0002.html	Есть
6.	Несанкционированный доступ в Cisco NX-OS	MITRE: CVE-2021-1361	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе , посредством отправки специально сформированных пакетов на порт 9075/tcp. Уязвимость обусловлена некорректной конфигурацией сервиса, привязанного к порту 9075/tcp.	24 февраля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021022417 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-3000-9000-fileaction-QtLzDRy2 https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvw89875	Есть
7.	Несанкционированный доступ в Cisco Application Services Engine	MITRE: CVE-2021-1393	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректным применением политик безопасности к сервисам, функционирующим в Data Network.	24 февраля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021022416 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-case-mvuln-dYrDPC6w https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvw14124	Есть
8.	Выполнение произвольного кода в WPE WebKit и WebKitGTK+	MITRE: CVE-2020-27918 MITRE: CVE-2020-9947	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия	22 марта 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021032301 https://webkitgtk.org/security/WSA-2021-0002.html	Есть

			пользователем специально созданной веб-страницы. Уязвимость обусловлена некорректной обработкой веб-контента.			
9.	Выполнение произвольного кода в Cisco SD-WAN	MITRE: CVE-2021-1433	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректной обработкой сетевого трафика процессом vDaemon.	24 марта 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021032415 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-buffover-CqdRWLc https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvu42778	Есть
10.	Выполнение произвольного кода в Visual Studio Code Python Extension	MITRE: CVE-2020-17163	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного файла. Уязвимость обусловлена некорректной проверкой входных данных.	17 марта 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021031701 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17163	Есть
11.	Уязвимость в плагине Paid Memberships Pro для WordPress	MITRE: CVE-2021-20678	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику посредством отправки специально сформированного SQL-запроса получить несанкционированный доступ к базе данных WordPress. Уязвимость обусловлена из-за некорректной очисткой предоставленных пользователем данных.	17 марта 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021031708 https://jvn.jp/en/jp/JVN08191557/index.html https://www.paidmembershipspro.com/pmpro-update-2-5-6/	Есть
12.	Выполнение произвольного кода в Adobe Connect	MITRE: CVE-2021-21085	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных.	9 марта 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021031001 https://helpx.adobe.com/security/products/connect/apsb21-19.html	Есть
13.	Выполнение произвольного кода в Microsoft Excel	MITRE: CVE-2021-27053	Эксплуатация уязвимости позволяет злоумышленнику выполнить произвольный код в целевой системе посредством открытия вредоносной страницы или вредоносного XLSфайла. Уязвимость обусловлена некорректной проверкой существования объекта перед выполнением операций с ним при обработке XLS-файлов.	9 марта 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021030940 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27053 https://www.zerodayinitiative.com/advisories/ZDI-21-332/	Есть
14.	Выполнение произвольного кода в Microsoft PowerPoint	MITRE: CVE-2021-27056	Эксплуатация уязвимости позволяет злоумышленнику выполнить произвольный код в целевой системе посредством открытия вредоносной страницы или вредоносного файла презентации. Уязвимость обусловлена некорректной проверкой существования объекта перед выполнением операций с ним при обработке файлов презентаций.	9 марта 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021030935 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27056	Есть
15.	Уязвимость в панели управления маршрутизаторов Cisco Small Business RV132W и RV134W	MITRE: CVE-2021-1287	Эксплуатация уязвимости позволяет удалённому аутентифицированному злоумышленнику выполнить произвольный код или вызвать отказ в обслуживании в целевой системе посредством отправки специально сформированного вредоносного HTTP-запроса.	17 марта 2021 г.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-132w134w-overflow-Pptt4H2p	Есть

			Уязвимости обусловлены некорректной обработкой HTTP-запросов в веб-панели управления уязвимого устройства.			
16.	Выполнение произвольного кода в Google Chrome	MITRE: CVE-2021-21191	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректным функционированием компонента WebRTC.	13 марта 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021031301 https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop_12.html https://crbug.com/1167357	Есть
17.	Выполнение произвольного кода в Google Chrome	MITRE: CVE-2021-21192	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректным определением границ памяти при группировании вкладок.	15 марта 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021031301 https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop_12.html https://crbug.com/1181387	Есть
18.	Выполнение произвольного кода в Google Chrome	MITRE: CVE-2021-21193	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректным функционированием компонента Blink.	15 марта 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021031301 https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop_12.html https://crbug.com/1186287	Есть