

ПРОМСВЯЗЬИНВЕСТ

расчетная небанковская кредитная организация

367000 РФ, Республика Дагестан, г. Махачкала, ул. Ирчи-Казака 2 «б»

ОКПО 43340114 БИК № 048209395 корсчет 301038109820900000395

тел.(8722) 62-16-24, 61-58-22 факс.(8722) 62-16-94 www.psib.ru E-mail: office@psib.ru

«04» апреля 2022г.

г. Махачкала

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за март 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 март 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 уязвимости	Описание уязвимости	Дата выявления	Ссылка на источники	Наличие обновлений
1.	Уязвимость нулевого дня в CMS Bitrix	ALRT-20220303.2	Эксплуатация уязвимости позволяет удаленному злоумышленнику записать произвольные файлы в уязвимую систему посредством отправки специально сформированных сетевых пакетов. Данная уязвимость присутствует в модуле «vote» CMS Bitrix.	3 марта 2022 г.	-	Есть
2.	Рекомендации по обеспечению безопасности телекоммуникационного оборудования	ALRT-20220305.1	В данных рекомендациях представлены сведения по базовым подходам к обеспечению информационной безопасности телекоммуникационного оборудования (управляемые коммутаторы, маршрутизаторы, межсетевые экраны, далее оборудование), а также его систем управления на участках сопряжения локальных вычислительных сетей предприятий с сетью Интернет, направленные на минимизацию рисков проведения компьютерных атак со стороны сети Интернет. 1. Обеспечить изоляцию каналов управления оборудованием и средств управления оборудованием от локально вычислительной сети предприятия. Рекомендуется организовать выделенную (логически изолированную) сеть управления, включающую средства управления и мониторинга технического состояния, ведения журналов событий, аутентификации пользователей. 2. По возможности отключить дистанционное управление оборудованием либо осуществлять такое управление по каналу, защищенному сертифицированными ФСБ России средствами криптографической защиты или организационно-техническими мерами (выделенный канал), исключающими возможность управления оборудованием кем либо кроме администратора. 3. Исключить несанкционированный доступ к управлению оборудованием. 4. Создать резервные копии программного обеспечения и	5 марта 2022 г.	-	Есть

			<p>конфигураций оборудования на внешних носителях. Вести учет изменений конфигураций.</p> <p>5. Ограничить доступ сторонних лиц, привлекаемых к обеспечению технического обслуживания, к системам управления оборудованием.</p> <p>6. Сменить пароли пользователей и администраторов оборудования и далее проводить такую смену не реже 1 раза в месяц. Устанавливаемые пароли должны соответствовать требованиям «сложности»:</p> <ul style="list-style-type: none"> - длина пароля должна быть не менее 12 символов; - пароль не должен основываться на словах естественного языка, а также на том, что связывает его с информацией личного характера (дата рождения, номер телефона и т.д.); - пароль не должен содержать более 2 следующих друг за другом одинаковых символов, в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, \$, %, * и т.п.) 			
3.	Уязвимость нулевого дня в Spring Framework	ALRT-20220331.1	<p>По каналам Национального координационного центра по компьютерным инцидентам получены сведения об уязвимости «нулевого дня» в одном из популярных фреймворков для разработки Java-приложений - Spring Framework.</p> <p>Обнаруженная уязвимость на данный момент не имеет идентификатора CVE, но носит название Spring4Shell. Указанное название присвоено по аналогии с наименованием уязвимости Log4Shell в виду схожести механизма внедрения исполняемого кода. Удаленный злоумышленник посредством отправки специально сформированных запросов может получить доступ к объекту AccessLogValve, отвечающему за создание журнала доступа к веб-серверу, переопределить параметры логирования и в последующем направить вредоносный запрос на создание JSP-файла, представляющего из себя удаленный исполняемый файл.</p>	31 марта 2022 г.	https://www.cyberkendra.com/2022/03/spring-shell-rce-0-day-vulnerability.html https://bugalert.org/content/notices/2022-03-29-spring.html https://github.com/BobTheShoplifter/Spring4Shell-POC https://www.springcloud.io/post/2022-03/spring-0day-vulnerability/#gsc.tab=0 https://websecured.io/blog/624411cf775ad17d72274d16/spring4shell-poc	Есть
4.	Выполнение произвольного кода в Cisco IOS and Cisco IOS XE	MITRE: CVE-2017-6736 CVE-2017-6737 CVE-2017-6738 CVE-2017-6739 CVE-2017-6740 CVE-	<p>Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного вредоносного SNMP-пакета через IPv4 или IPv6. Уязвимость</p>	03 июля 2017 г.	https://www.cybersecurity-help.cz/vdb/SB2017070303 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp	Есть

		2017-6741 CVE-2017-6742 CVE-2017-6743 CVE-2017-6744	обусловлена некорректной проверкой входных данных.			
5.	Множественные уязвимости в ПО IBM	MITRE: CVE-2021-41035	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректными ограничениями доступа.	08 марта 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022030806 https://www.cybersecurity-help.cz/vdb/SB2022030803 http://www.ibm.com/blogs/psirt/security-bulletin-multiple-vulnerabilities-in-sterling-connectdirect-browser-user-interface/ http://www.ibm.com/support/pages/node/6561041 http://www.ibm.com/blogs/psirt/security-bulletin-some-unspecified-vulnerabilities-in-java-se-result-in-the-unauthenticated-attacker-to-take-control-of-the-system-or-some-impact/ http://www.ibm.com/support/pages/node/6561577	Есть
6.	Множественные уязвимости в ПО IBM	MITRE: CVE-2021-35560	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных.	08 марта 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022030806 https://www.cybersecurity-help.cz/vdb/SB2022030803 http://www.ibm.com/blogs/psirt/security-bulletin-multiple-vulnerabilities-in-sterling-connectdirect-browser-user-interface/ http://www.ibm.com/support/pages/node/6561041 http://www.ibm.com/blogs/psirt/security-bulletin-some-unspecified-vulnerabilities-in-java-se-result-in-the-unauthenticated-attacker-to-take-control-of-the-system-or-some-impact/ http://www.ibm.com/support/pages/node/6561577	Есть
7.	Выполнение произвольных команд ОС в Zyxel NWA1100-NH	MITRE: CVE-2022-25312	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды ОС в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных.	07 марта 2022 г.	http://www.zyxel.com/support/OS-command-injection-vulnerability-of-NWA1100-NH-access-point.shtml https://www.cybersecurity-help.cz/vdb/SB2022030704	Есть
8.	Выполнение произвольного кода в Linux kernel	MITRE: CVE-2022-25312	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена использованием неинициализированных ресурсов.	08 марта 2022 г.	http://dirtypipe.cm4all.com/ https://www.cybersecurity-help.cz/vdb/SB2022030808	Есть
9.	Выполнение произвольного кода в Microsoft Remote Desktop Client	MITRE: CVE-2022-21990 CVE-2022-23285	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных.	08 марта 2022 г.	http://portal.msrm.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21990 http://portal.msrm.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23285 https://www.cybersecurity-help.cz/vdb/SB2022030814	Есть
10.	Выполнение произвольного кода в Adobe Illustrator	MITRE: CVE-2022-23187	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.	09 марта 2022 г.	http://helpx.adobe.com/security/products/illustrator/apsb22-15.html https://www.cybersecurity-help.cz/vdb/SB2022030903	Есть
11.	Выполнение произвольного кода в Microsoft Exchange Server	MITRE: CVE-2022-23277	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса.	08 марта 2022 г.	http://portal.msrm.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23277 https://www.cybersecurity-help.cz/vdb/SB2022030818	Есть

			Уязвимость обусловлена некорректной проверкой входных данных.			
12.	Выполнение произвольного кода в Adobe Photoshop	MITRE: CVE-2022-24090	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.	09 марта 2022 г.	http://helpx.adobe.com/security/products/photoshop/apsb22-14.html https://www.cybersecurity-help.cz/vdb/SB2022030902	Есть
13.	Множественные уязвимости в Microsoft .NET and Visual Studio	MITRE: CVE-2022-24512	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных.	08 марта 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022030847 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24512 http://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-24464	Есть
14.	Множественные уязвимости в Microsoft .NET and Visual Studio	MITRE: CVE-2022-24464	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить отказ в обслуживании целевой системы посредством отправки специально сформированных данных. Уязвимость обусловлена ошибкой границ памяти.	08 марта 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022030847 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24512 http://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-24464	Есть
15.	Множественные уязвимости в Mozilla Firefox и Firefox ESR	MITRE: CVE-2022-26381 CVE-2022-26385	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством изменения текста в объекте SVG. Уязвимость обусловлена ошибкой использования после освобождения.	08 марта 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022030807 http://www.mozilla.org/en-US/security/advisories/mfsa2022-10/ http://www.mozilla.org/en-US/security/advisories/mfsa2022-11/	Есть
16.	Множественные уязвимости в Mozilla Firefox и Firefox ESR	MITRE: CVE-2022-0843	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти.	08 марта 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022030807 http://www.mozilla.org/en-US/security/advisories/mfsa2022-10/ http://www.mozilla.org/en-US/security/advisories/mfsa2022-11/	Есть
17.	Выполнение произвольного кода в Mozilla Firefox	MITRE: CVE-2022-26485 CVE-2022-26486	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 марта 2022 г.	http://www.mozilla.org/en-US/security/advisories/mfsa2022-09/ https://www.cybersecurity-help.cz/vdb/SB2022030501	Есть
18.	Выполнение произвольного кода в D-Link Router DIR-810L, DIR-820L, DIR-830L, DIR-826L, DIR-836L	MITRE: CVE-2021-45382	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных.	25 февраля 2022 г.	https://github.com/doudoudedi/D-LINK_Command_Injection1/blob/main/D-LINK_Command_injection.md https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10264 https://nvd.nist.gov/vuln/detail/CVE-2021-45382	Есть
19.	Выполнение произвольного кода в D-Link Router DIR-846	MITRE: CVE-2021-46314	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных.	25 февраля 2022 г.	https://www.dlink.com/en/security-bulletin/ https://github.com/doudoudedi/DIR-846_Command_Injection/blob/main/DIR-846_Command_Injection1.md https://www.tenable.com/cve/CVE-2021-46314 https://www.opencve.io/cve/CVE-2021-46314	
20.	Множественные уязвимости в Microsoft Edge	MITRE: CVE-2022-0800	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством	04 марта 2022 г.	http://crbug.com/1294097 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0794 http://chromereleases.googleblog.com/2022/0	Есть

			открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти.		3/stable-channel-update-for-desktop.html http://crbug.com/1282782 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0795 http://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html http://crbug.com/1295786 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0796 http://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html http://crbug.com/1281908 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0797 http://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html http://crbug.com/1289383	
21.	Множественные уязвимости в Microsoft Edge	MITRE: CVE-2022-0801 CVE-2022-0802 CVE-2022-0803 CVE-2022-0804 CVE-2022-0807	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной реализацией проверок безопасности.	04 марта 2022 г.	http://crbug.com/1294097 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0794 http://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html http://crbug.com/1282782 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0795 http://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html http://crbug.com/1295786 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0796 http://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html http://crbug.com/1281908 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0797 http://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html http://crbug.com/1289383	Есть
22.	Множественные уязвимости в Google Chrome	MITRE: CVE-2022-0800	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти.	04 марта 2022 г.	http://crbug.com/1294097 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0794 http://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html http://crbug.com/1282782 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0795 http://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html http://crbug.com/1295786 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0796 http://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop.html http://crbug.com/1281908	Есть
23.	НСД в several Zyxel firewalls	MITRE: CVE-2022-0342	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректной работой процесса аутентификации.	30 марта 2022 г.	http://www.zyxel.com/support/Zyxel-security-advisory-for-authentication-bypass-vulnerability-of-firewalls.shtml	Есть