

# 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](http://www.psib.ru) E-mail: office@psib.ru

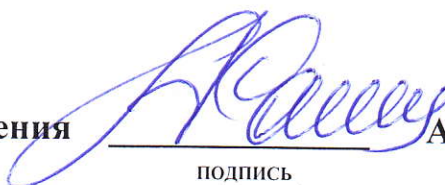
«05» сентября 2022г.

г. Махачкала

## «Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за август 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 август 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.	Множественные уязвимости в Linux Kernel	MITRE: CVE-2022-1679	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнить произвольный код с привилегиями «root» в целевой системе. Уязвимость обусловлена ошибкой использования после освобождения.	02 августа 2022 г.	<a href="https://ubuntu.com/security/notices/USN-5544-1">https://ubuntu.com/security/notices/USN-5544-1</a>	Есть
2.	Множественные уязвимости в Linux Kernel	MITRE: CVE-2022-1652	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику вызвать отказ в обслуживании целевой системы посредством запуска специально созданной вредоносной программы. Уязвимость обусловлена ошибкой использования после освобождения.	02 августа 2022 г.	<a href="https://ubuntu.com/security/notices/USN-5544-1">https://ubuntu.com/security/notices/USN-5544-1</a>	Есть
3.	Множественные уязвимости в Linux Kernel	MITRE: CVE-2022-28893	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнить произвольный код с привилегиями «root» в целевой системе. Уязвимость обусловлена ошибкой использования после освобождения.	02 августа 2022 г.	<a href="https://ubuntu.com/security/notices/USN-5544-1">https://ubuntu.com/security/notices/USN-5544-1</a>	Есть
4.	Выполнение произвольного кода в Chrome OS	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.	11 августа 2022 г.	<a href="http://chromereleases.googleblog.com/2022/08/long-term-support-channel-update-for.html">http://chromereleases.googleblog.com/2022/08/long-term-support-channel-update-for.html</a>	Есть
5.	Повышение привилегий в Kaspersky VPN Secure Connection	MITRE: CVE-2022-27535	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена небезопасным переходом по ссылке при удалении папок.	5 августа 2022 г.	<a href="http://www.synopsys.com/blogs/software-security/cyrc-advisory-kaspersky-vpn-microsoft-windows/">http://www.synopsys.com/blogs/software-security/cyrc-advisory-kaspersky-vpn-microsoft-windows/</a>	Есть
6.	Множественные уязвимости в Microsoft Edge	MITRE: CVE-2022-33649	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой при обработке HTML-содержимого.	5 августа 2022 г.	<a href="http://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html">http://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html</a> <a href="http://crbug.com/1320538">http://crbug.com/1320538</a> <a href="http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-2611">http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-2611</a> <a href="http://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html">http://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop.html</a> <a href="http://crbug.com/1330489">http://crbug.com/1330489</a> <a href="http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-2606">http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-2606</a>	Есть



7.	Множественные уязвимости в Adobe Illustrator	MITRE: CVE-2022-34260	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.	10 августа 2022 г.	<a href="http://helpx.adobe.com/security/products/illustrator/apsb22-41.html">http://helpx.adobe.com/security/products/illustrator/apsb22-41.html</a>	Есть
8.	Множественные уязвимости в Adobe Acrobat	MITRE: CVE-2022-35665	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.	10 августа 2022 г.	<a href="http://helpx.adobe.com/security/products/acrobat/apsb22-39.html">http://helpx.adobe.com/security/products/acrobat/apsb22-39.html</a>	Есть
9.	Множественные уязвимости в Adobe Acrobat	MITRE: CVE-2022-35666	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного PDF-файла. Уязвимость обусловлена некорректной проверкой входных данных.	10 августа 2022 г.	<a href="http://helpx.adobe.com/security/products/acrobat/apsb22-39.html">http://helpx.adobe.com/security/products/acrobat/apsb22-39.html</a>	Есть
10.	Выполнение произвольного кода в Zlib	MITRE: CVE-2022-37434	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.	7 августа 2022 г.	<a href="https://github.com/nodejs/node/blob/75b68c64db515f76df73af476eccc382bbcb00a/deps/zlib/inflate.c#L762-L764">https://github.com/nodejs/node/blob/75b68c64db515f76df73af476eccc382bbcb00a/deps/zlib/inflate.c#L762-L764</a> <a href="https://github.com/ivd38/zlib_overflow">https://github.com/ivd38/zlib_overflow</a>	Есть
11.	Отказ в обслуживании в Foxit PDF Reader и Foxit PDF Editor	Не определен	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызывать отказ в обслуживании целевой системы посредством открытия пользователем специально созданного вредоносного PDF-файла. Уязвимость обусловлена некорректной проверкой входных данных.	29 июля 2022 г.	<a href="http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Reader+12.0.1+and+Foxit+PDF+Editor+12.0.12022-07-29+00%3A00%3A00">http://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Reader+12.0.1+and+Foxit+PDF+Editor+12.0.12022-07-29+00%3A00%3A00</a>	Есть
12.	Выполнение произвольного кода в Mozilla Thunderbird	MITRE: CVE-2022-2505	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти.	29 июля 2022 г.	<a href="http://www.mozilla.org/en-US/security/advisories/mfsa2022-32/">http://www.mozilla.org/en-US/security/advisories/mfsa2022-32/</a>	Есть