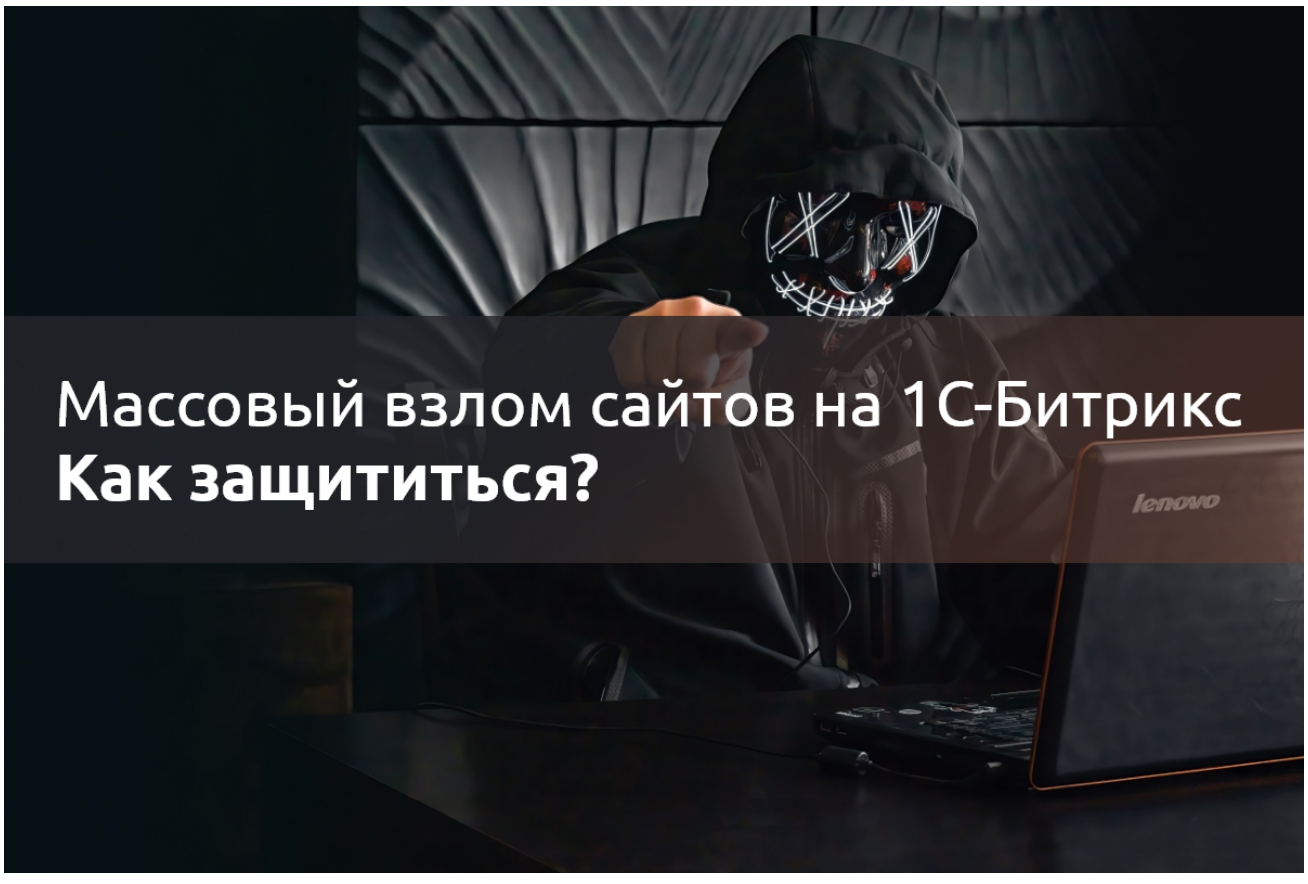
Массовый взлом сайтов на 1С-Битрикс. Как защититься?

Опубликовано: 30 Июня 2022 **Изменено:** 29 Октября 2022 **Время чтения:** 7 минут 14 371



За последний месяц участились случаи взломов сайтов на 1С-Битрикс и Битрикс24.

> Статья будет дополняться. Добавьте в закладки, чтобы не потерять.

28 июня 2022 года (в день независимости Украины) появились сообщения о взломе десятков сайтов (точные цифры неизвестны). Вот так стали выглядеть взломанные ресурсы:

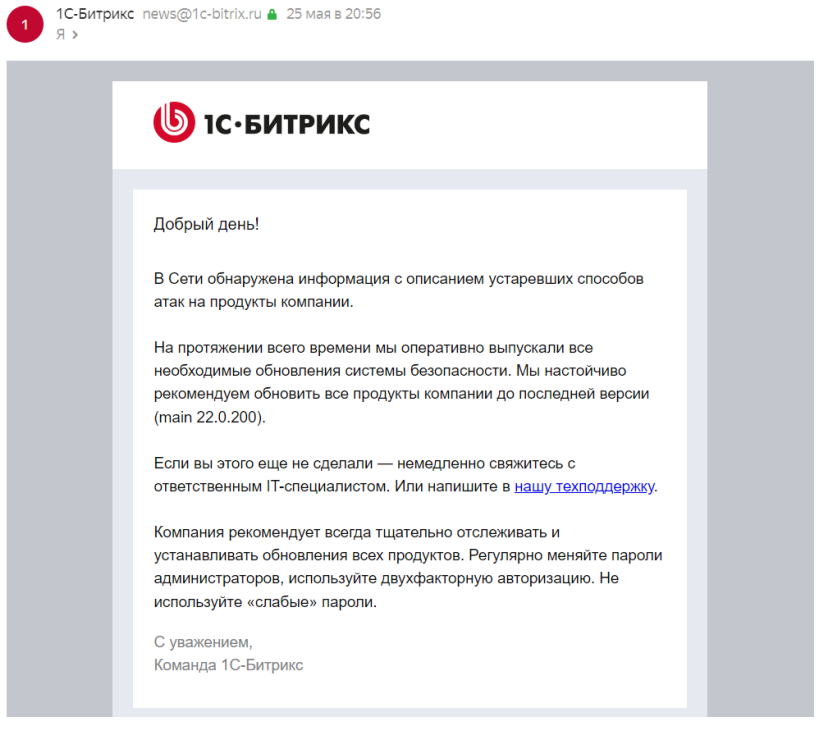
День Конституции – один из важнейших праздников для любого государства, функционирующего в демократическом и законном поле. Конституция – важнейший инструмент, который позволяет руководству страны работать во благо своего народа, а нарушение этого документа или попытка его переписать и отменить – тяжелейшее преступление, наказуемое по всей строгости закона.

Российские граждане солидарны с украинским народом в его борьбе за независимость и собственный, Украино-ориентированный законодательный фундамент. Мы надеемся на скорейшую нормализацию ситуации в стране, которая резко ухудшилась после начала специальной военной операции руководством России.

Российские чиновники и общественные деятели готовы помогать в восстановлении Украины всеми возможными способами и выражают искреннее сожаление в связи с развязанной руководством России войной.

С Днем Конституции, Украина. Демократия обязательно одержит верх!

Надо отдать должное, 1С-Битрикс закрыл все известные уязвимости еще в мае и разослал информационные письма. Так что взлому подвержены только сайты на старых версиях CMS.


1С-Битрикс news@1c-bitrix.ru 25 мая в 20:56
Я

1С·БИТРИКС

Добрый день!

В Сети обнаружена информация с описанием устаревших способов атак на продукты компании.

На протяжении всего времени мы оперативно выпускали все необходимые обновления системы безопасности. Мы настойчиво рекомендуем обновить все продукты компании до последней версии (main 22.0.200).

Если вы этого еще не сделали — немедленно свяжитесь с ответственным IT-специалистом. Или напишите в нашу техподдержку.

Компания рекомендует всегда тщательно отслеживать и устанавливать обновления всех продуктов. Регулярно меняйте пароли администраторов, используйте двухфакторную авторизацию. Не используйте «слабые» пароли.

С уважением,
Команда 1С-Битрикс

В официальном заявлении 1С-Битрикс также говорит об отсутствии уязвимостей в актуальной версии CMS.

Как обновить 1С-Битрикс самостоятельно

Если вы еще не обновили свой битрикс, крайне советуем это сделать. Если вдруг вы поддерживаете сайт своими силами, напомню порядок действий:

1. Обновить можно сайт только на активной лицензии. Да, придется покупать продление, если у вас его нет.
2. Сделайте свежий бэкап сайта (проверьте его наличие).
3. По возможности разверните резервную копию на тестовом сервере и обновите сайт там.
4. Если вы уверены, что обновления у вас проходят без проблем, в ядро вы не вмешивались, а весь код поддерживает PHP 7.4 – обновляйте.
5. Если нужно обновить PHP и MySQL до актуальных версий – обновляйте. Предварительно лучше сделать бэкап на уровне сервера / хостинга.
6. Проверьте работоспособность всех разделов сайта.

Как еще обезопасить сайт?

Универсальные рекомендации следующие:

- Периодически меняйте пароли.
- Настройте регулярное резервное копирование в облако. Резервные копии в папке сайта легко удалить.
- Деактивируйте административные аккаунты, если вы не знаете кому они принадлежат или если сотрудник уже не работает у вас.
- Просканируйте сайт на наличие уязвимостей с помощью встроенного функционала Битрикса.

Понимаем, что не все читатели статьи технические специалисты, поэтому давайте вкратце расскажем про основные моменты.

Смените пароли

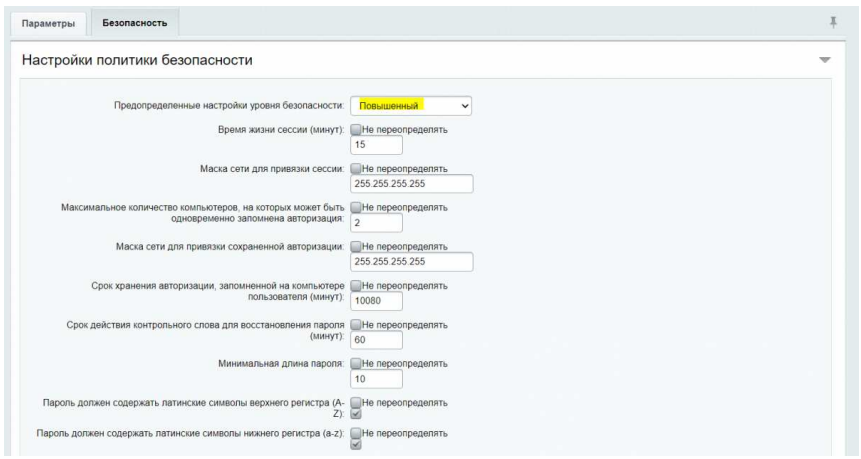
Поменяйте пароли не только Администраторов, но и всех, кто имеет доступ к админке (контент-менеджеры, администраторы магазина и т.д.).

Пароли должны быть сложными: не менее 8 символов, а также должны содержать буквы в разном регистре, цифры и символы.

Смените пароль к Хостингу и к FTP/SFTP аккаунтам. Это можно сделать в настройках Хостинга.

Повысьте уровень безопасности Администраторов

Установите “Повышенный” уровень безопасности администраторов.



Сделать это можно на странице: Настройки - Пользователи - Группы пользователей. Далее переходите в редактирование группы “Администраторы”.

Включите встроенную в 1С-Битрикс защиту

Включите Проактивную защиту: Настройки – Проактивная защита – Проактивный фильтр.

Включите Веб-антивирус: Настройки – Проактивная защита – Веб-антивирус.

Включите защиту сессий: Настройка – Проактивная защита – Защита сессий.

Включите защиту от редиректов: Настройка – Проактивная защита – Защита редиректов.

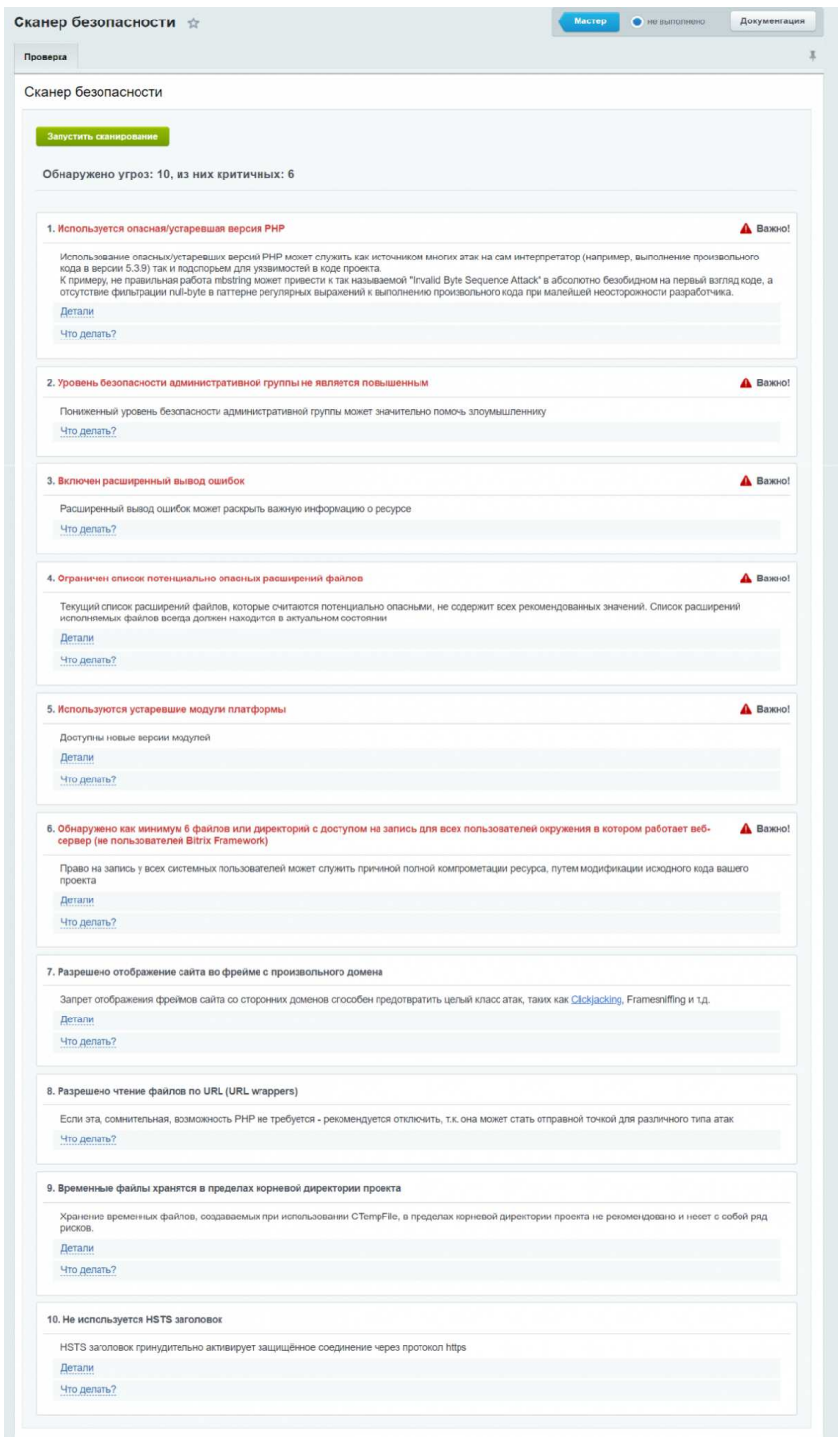
Включите защиту от фреймов: Настройка – Проактивная защита – Защита от фреймов.

Если у вас используется статический IP, включите защиту Административного раздела: Настройки – Проактивная защита – Защита административного раздела.

Если возможно, включите двухфакторную авторизацию.

Просканируйте сайт на наличие уязвимостей

Зайдите в Настройки – Проактивная защита – Сканер безопасности и запустите сканирование.



Смотрите какие тесты сайт не прошел и выполните рекомендации. Также рекомендации можно посмотреть тут: Настройки – Проактивная защита – Панель безопасности.

Установите модуль “Поиск троянов” из Маркетплейса: https://marketplace.1c-bitrix.ru/solutions/bitrix.xscan/

Просканируйте сайт и устраните недочеты. После установки модуль можно найти здесь: Настройки – bitrix.xscan – Поиск троянов.

Поищите файлы, которые были изменены недавно. Если есть доступ к консоли, это можно сделать командой:

```
find . -type f -printf '%TY-%Tm-%Td %TT %p\n' | sort -r
```

Проверяем каждый файл из списка вручную.

Удалите файл /bitrix/tools/putin_***lo.php

Проверьте агенты на наличие подозрительных записей

Переходите в Настройки – Настройки продукта – Агенты.

Удалите подозрительные.

Что делать если уже взломали и нет доступа в админку?

Мы писали как можно авторизоваться под администратором без пароля в этой статье: https://ydmitry.ru/blog/avtorizatsiya-pod-adminom-bez-logina-i-parolya-v-bitrix/.

Восстановить сломанный сайт зачастую намного сложнее, чем обезопасить его от взлома. Самое простое решение: развернуть сайт из последней резервной копии, после чего проделать все рекомендации выше.

Если резервных копий 1С-Битрикс нет – попробуйте запросить резервную копию у Хостера. Если и такой нет – скорее всего придется восстанавливать сайт вручную. Как правило, удаляют файлы /bitrix/.settings.php и /bitrix/php_interface/dbconn.php, изменяют главную страницу, удаляют инфоблоки. Перед восстановлением обязательно обезопасьте сайт, иначе результат многочасовой работы будет спущен в унитаз.

Что если обновить Битрикс нельзя?

Бывает, что проект давно не обновлялся, не поддерживает актуальную версию PHP, были внесены изменение в ядро или сайт падает после обновления по непонятным причинам, а разбираться нет времени.

В данный момент взлом идет через модуль vote. Существует три способа защиты.

Первый способ: вставляем код в файлы

- /bitrix/tools/upload.php
- /bitrix/tools/mail_entry.php
- /bitrix/modules/main/include/virtual_file_system.php
- /bitrix/components/bitrix/sender.mail.editor/ajax.php
- /bitrix/tools/vote/uf.php
- /bitrix/tools/html_editor_action.php
- /bitrix/admin/site_checker.php

перед required:

```
if ($_SERVER['REQUEST_METHOD'] === 'POST') {
        header("Status: 404 Not Found");
        die();
}
```

Второй способ: ограничить на уровне nginx. Вариант для тех, у кого свой сервер.

```
# ломает загрузку файлов в ИБ
location /bitrix/tools/upload.php {
        if ($request_method = POST ) {
            deny all;
        }
}

location /bitrix/tools/mail_entry.php {
        if ($request_method = POST ) {
            deny all;
        }
}

location /bitrix/tools/vote/uf.php {
        if ($request_method = POST ) {
            deny all;
        }
}

location /bitrix/tools/html_editor_action.php {
        if ($request_method = POST ) {
            deny all;
        }
}

location /bitrix/admin/site_checker.php {
        if ($request_method = POST ) {
            deny all;
        }
}
```

Третий способ: защита с помощью .htaccess. Подойдет тем, у кого Хостинг. В директориях, в которых лежат уязвимые файлы создаем файлы .htaccess (если их нет) и прописываем конструкцию:

```
<Files ~ "^(имя файлов)\.php$>
    deny from all
</Files>
```

Вместо “имя файлов” – пишите список уязвимых файлов в данной директории, разделенных символом “|” (без кавычек).

Для /bitrix/tools/:

```
<Files ~
"^(html_editor_action|mail_entry|upload)\.php$>
    deny from all
</Files>
```

Для /bitrix/tools/vote/:

```
<Files ~ "^(uf)\.php$>
    deny from all
</Files>
```

Для /bitrix/modules/main/include/:

```
<Files ~ "^(virtual_file_system)\.php$>
    deny from all
</Files>
```

Для /bitrix/components/bitrix/sender.mail.editor/:

```
<Files ~ "^(ajax)\.php$>
    deny from all
</Files>
```

Для /bitrix/admin/:

```
<Files ~ "^(site_checker)\.php$>
    deny from all
</Files>
```

Внимание: решение временное, часть функционала админки сайта при использовании любого из трех методов будет недоступна.

Заключение

Актуальную информацию можно посмотреть в этой ветке: https://dev.1c-bitrix.ru/support/forum/forum6/topic147346/

Описание уязвимости: https://bdu.fstec.ru/vul/2022-01141

Если возникнут проблемы с восстановлением, обновлением или защитой сайта – пишите нам, поможем решить вашу проблему.

#1С-Битрикс #Безопасность #Руководство #Вирусы

Дмитрий Языков

10+ лет в Digital. Пишу про автоматизацию бизнеса, маркетинг и дизайн.

Участвует в подборках:

Вам понравятся статьи:

Как мы спасали сайт на 1С-Битрикс от баннерного вируса

Авторизация под админом без логина и пароля в 1С-Битрикс

7 смертных грехов разработки на 1С-Битрикс

Как перенести сайт на 1С-Битрикс на другой

хостинг

80 каналов привлечения трафика

Нужен сайт или продвижение? Проконсультируем в Телеграм или Whatsapp

Подпишись на наш Телеграм канал →

Yazykov Digital

ИП Языков Д.В.
ИНН: 164493749152
ОГРНИП: 319169000175546