TLP: GREEN

Рекомендации
по применению компенсирующих мер и реагированию на атаки, связанные с CMS «1С-Битрикс: Управление сайтом»

www.cyberok.ru

15 июля 2023 г.

Версия 1.4

Оглавление

Оглавление....2
1 Общая информация....3
2 Используемые уязвимости....5
2.1 Arbitrary Object Instantiation в модуле «Опросы, голосования»/«Vote»....5
2.2 Arbitrary File Write в модуле «Визуальный редактор»....6
3 Описание действий постэксплуатации....7
4 Описание реагирования на успешную атаку....8
4.1 Идентификация....8
4.1.1 Проверка средствами «1С-Битрикс:Поиск троянов»....8
4.1.2 Проверка по журналам доступа к WEB-серверу....8
4.1.3 Поиск новых вредоносных файлов....9
4.1.4 Поиск модифицированных файлов....10
4.1.5 Поиск закрепления доступа....11
4.2 Сдерживание....12
4.2.1 Модификация файлов WEB-приложения....13
4.2.2 Ограничение доступа к уязвимым файлам средствами WEB-сервера....13
4.2.3 Ограничение доступа к уязвимым файлам средствами WAF/NGFW....13
5 Очистка зараженного узла и восстановление приложения....14
6 Рекомендации по защите WEB-приложения....15
7 Восстановление работоспособности в случае блокировки....16
8 Контакты....16

1 Общая информация

26.05.2023 был проведен массовый дефейс веб-серверов национального сегмента РФ сети Интернет.

В качестве цели атаки выступала CMS 1C Bitrix. В ходе расследования было установлено, что массовые взломы были проведены загодя, начиная с 2022 года через известные уязвимости, включая CVE-2022-27228.
Злоумышленником был установлен бэкдор, позволяющий создавать произвольные файлы и вызывать команды ОС. 26 мая в районе 14:00 бэкдору была дана команда на замену главной страницы сайта. Техническое описание атаки было опубликовано на форуме разработчиков.

Зачастую взломанные сайты восстанавливаются из резервной копии, но это не решает проблему, поскольку восстанавливается и бэкдор, что дает возможность злоумышленнику повторить атаку.
Кроме того, если уязвимость не была устранена, злоумышленники могут снова взломать сервер и установить модификацию бэкдора, что наблюдается в настоящий момент.

Целью атак являются:

- Все не обновленные версии «1С-Битрикс: Управление сайтом» (Bitrix Site Manager). Следует обратить внимание, что после окончания срока действия лицензии, обновление ПО не выполняется.
- Обновленные версии «1С-Битрикс: Управление сайтом» с незакрытыми уязвимостями.
- Обновленные версии «1С-Битрикс: Управление сайтом» с установленным бэкдором.

13.07.2023 были выявлены артефакты, подтверждающие установку keylogger на скомпрометированные узлы. После компрометации узла выполняется модификация файла панели управления CMS 1C Bitrix (/bitrix/admin/index.php). В начало файла дописывается вызов функции "file_put_contents(..., print_r($_REQUEST,1))".

В результате в "/bitrix/tools/" создаётся скрытый файл ".sess" (“.idSess” или “.session”), в который записываются все попытки аутентификации (в том числе логин, пароль и session cookie). Дополнительная опасность в том, что в журнал keylogger могут записываться также session cookie для других веб-приложений, существующих на том же домене, что и скомпрометированная CMS 1C Bitrix. В таком случае злоумышленник получает доступ не только к административной панели Bitrix, но и валидную сессию для других веб-приложений.

2 Используемые уязвимости

2.1 Arbitrary Object Instantiation в модуле «Опросы, голосования»/«Vote»

Модуль «Опросы, голосования» («Vote») позволяет проводить опросы и голосования, которые помогают узнать мнение пользователей сайта.

Эксплуатация уязвимости позволяет удаленному злоумышленнику записать произвольные файлы в систему посредством отправки специально сформированных сетевых пакетов. Данная уязвимость присутствует в модуле «vote» CMS «1С-Битрикс: Управление сайтом» до версии 22.0.400 всех редакций, кроме «Старт».

Общее описание уязвимости представлено по следующим ссылкам:

- https://bdu.fstec.ru/vul/2022-01141
- https://safe-surf.ru/upload/ALRT/ALRT-20220712.1.pdf
- https://helpdesk.bitrix24.com/open/15536776/

17.03.2022 уязвимости был присвоен номер CVE-2022-27228.

23.05.2022 в публичном доступе появился документ «attacking_bitrix.pdf», где разбирались новые уязвимости в CMS «1С-Битрикс» и методы их эксплуатации, включая CVE-2022-27228. В этом документе описан способ эксплуатации уязвимости CVE-2022-27228, приводящий к выполнению произвольных команд неавторизованным пользователем.

Если на WEB-сервере включено логирование POST-запросов, то в результате успешной эксплуатации CVE-2022-27228 в лог файл запишется строка, содержащая успешный POST-запрос к файлу «/bitrix/tools/vote/uf.php».

Пример:

```
***POST
/bitrix/tools/vote/uf.php?attachId[ENTITY_TYPE]=CFileUploader&attachId[ENTITY_ID][events][onFileIsStarted][]=CAllAgent&attachId[ENTITY_ID][events][onFileIsStarted][]=Update&attachId[MODULE_ID]=vote&action=vote HTTP/1.0" 200 ***
```

2.2 Arbitrary File Write в модуле «Визуальный редактор»

В основную кодовую базу «1С-Битрикс: Управление сайтом» входит служебный модуль «fileman», реализующий возможность визуального HTML-редактора. В составе этого модуля присутствует уязвимый скрипт «html_editor_action.php». Эксплуатация уязвимости этого файла аналогично CVE-2022-27228 позволяет неавторизованному Злоумышленнику удаленно выполнять произвольный код на целевой системе.

В результате успешной эксплуатации этой уязвимости, в лог файле появится строка, содержащая успешный POST-запрос к файлу «/bitrix/tools/html_editor_action.php»

Пример:

***POST /bitrix/tools/html_editor_action.php HTTP/1.0" 200 ***

3 Описание действий постэксплуатации

Основные действия после эксплуатации:

- замена index.php в корневой директории WEB-приложения;
- встраивание вредоносного кода в PHP-скрипты модулей;
- встраивание вредоносного кода в файл /bitrix/admin/index.php;
- удаление файла /bitrix/.settings.php;
- создание скриптов Агентов с вредоносным кодом или модификация существующих скриптов;
- удаление данных из таблиц базы данных b_iblock, b_iblock_element, b_iblock_element_property;
- создание файлов .htaccess во всех каталогах WEB-приложения;
- создание PHP-скриптов в директории /bitrix/admin/ с произвольными именами файлов;
- и т. д.

4 Описание реагирования на успешную атаку

4.1 Идентификация

4.1.1 Проверка средствами «1С-Битрикс:Поиск троянов»

Необходимо установить из каталога готовых решений «1С-Битрикс:Поиск троянов» и запустить сканирование. Для этого необходимо открыть панель управления сайта и перейти на следующую вкладку:

Настройки → bitrix.xscan → Поиск и Поиск (бета).

Модуль отсканирует весь сайт и отобразит выявленные подозрительные файлы.

4.1.2 Проверка по журналам доступа к WEB-серверу

Проверить факт успешной эксплуатации CVE-2022-27228.

Пример команды поиска:

```
grep -E 'POST /bitrix/tools/(html_editor_action.php)|(vote/uf.php)' /var/log/www.access.log*  | grep ' 200 '
```

Аналогичным образом проверить запросы к файлам из Таблицы №2 с кодом ответа 200.

Аналогичным образом проверить POST-запросы с кодом ответа 200, содержащие строки:

Фрагмент строки
bitrixxx
BX_STAT
BX_TOKEN
==

Для поиска ‘BX_STAT’ лучше воспользоваться регулярным выражением:

‘BX_STAT[^E]’

Так как аргумент ‘BX_STATE’ используется по умолчанию в легитимных файлах.

4.1.3 Поиск новых вредоносных файлов

1. Проверить наличие нетипичных файлов. Были выявлены следующие индикаторы компрометации:

Имя файла	Директория	Пример команды для поиска
xmlrpcs.php	Используются различные каталоги	find ./ -name xmlrpcs.php
inputs.php	Используются различные каталоги	find ./ -name inputs.php рекомендуется исключить из поиска легитимный файл: /bitrix/modules/sale/lib/delivery/inputs.php
l.php	/bitrix/src/app/	find ./ -name l.php
/bitrix/tools/spread.php	/bitrix/tools/ /bitrix/	
access.php wp.php term.php locale.php themes.php network.php container.php router.php wp-login.php	/bitrix/modules/iblock/lib/ bizproctype/	любой из файлов в указанной директории
/bitrix/tools/send_trait_imap.php		
/bitrix/tools/.cas.php /bitrix/tools/.cas.tmp.php		
/bitrix/tools/seo_page_ajax.php	/bitrix/tools/	find ./ -name seo_page_ajax.php
.sess .idSess .session	/bitrix/tools/	find / -name '.sess' -o -name '.idSess' -o -name '.session'

Таблица №2. Индикаторы компрометации

2. Рекомендуется обратить внимание на все файлы с несловарным, случайно сгенерированным именем из набора символов [a-z, 0-9] в каталоге /bitrix/admin/ и в корневой директории сайта.

Были выявлены файлы вида:

/bitrix/admin/f408f2b7df70.php

/bitrix/admin/8f1c222aae51.php

/2469a41bac71.php

/98826/bfd99.php

4.1.4 Поиск модифицированных файлов

Кроме создания новых файлов, злоумышленники могут вносить изменения в существующие файлы с целью встраивания вредоносного кода. Для этого необходимо проверить наличие в исходном коде приложения фрагментов строк из Таблицы №3.

Фрагмент строки
str_rot13
md5($_COOKIE
bitrixxx
eval(base64_decode
BX_STAT
BX_TOKEN
parse_str(hex2bin
iasfgjlzcb
QlhfVE9LRU4=
gzinflate(base64_decode
C.A.S
urldecode(base64_decode(hex2bin
print_r($_REQUEST,1))

Таблица №3

Из результатов поиска по «str_rot13» необходимо исключить следующие файлы:

/bitrix/modules/main/classes/general/vuln_scanner.php

/bitrix/modules/main/lib/search/content.php

/bitrix/modules/socialnetwork/lib/item/logindex.php

В этих файлах функция «str_rot13()» используется по умолчанию.

Для поиска файлов с ‘BX_STAT’ лучше воспользоваться регулярным выражением вида:

‘BX_STAT[^E]

Так как аргумент ‘BX_STATE’ используется по умолчанию в легитимных файлах.

Пример команды для поиска подозрительных файлов:

```
grep -Er 'str_rot13|md5\(\$_COOKIE|bitrixxx|eval\(base64_decode|BX_STAT[^E]|BX_TOKEN|parse_str\(hex2bin|iasfgjlzcb|QlhfVE9LRU4=|gzinflate\(base64_decode|C\.A\.S|urldecode\(base64_decode\(hex2bin|print_r\(\$_REQUEST\,1' /*
```

Известные файлы, в которые встраивается вредоносный код:

/bitrix/modules/main/include/prolog_after.php
/bitrix/admin/security_file_verifier.php
/bitrix/modules/main/bx_root.php
/bitrix/admin/index.php

Следует обратить внимание, что искать стоит не только по файлам приложения (php), так как злоумышленники в том числе используют технику с записью файла “.htaccess” для изменения конфигурации веб-сервера.

4.1.5 Поиск закрепления доступа

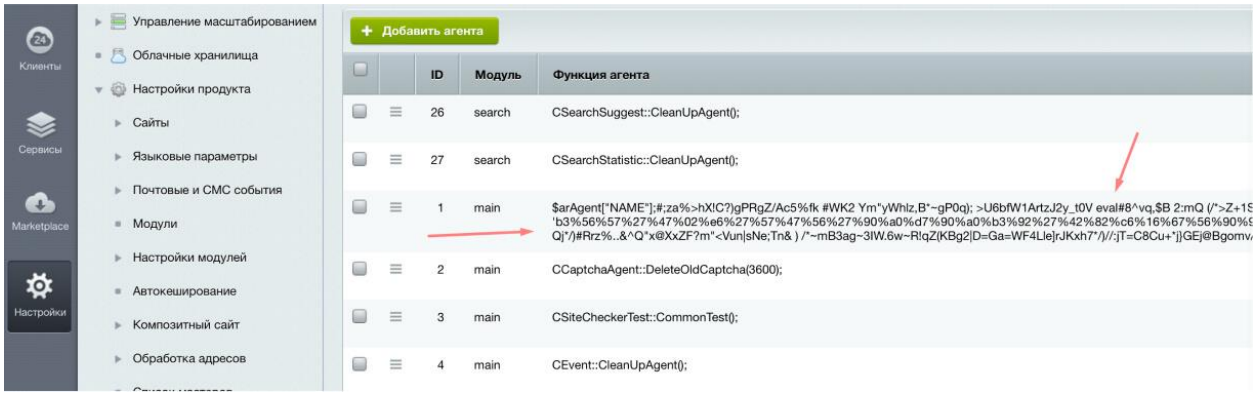
1. Проверить планировщик задач (cron) на наличие нелегитимных задач:

```
ls /etc/cron*
```

2. На странице со списком Агентов «1С-Битрикс» (/bitrix/admin/agent_list.php) проверить вызываемые функции на наличие вредоносного кода.
Для этого необходимо открыть панель управления сайта и перейти на следующую вкладку:

Настройки > Настройки продукта > Агенты

Название агента может быть любым, но, скорее всего, вредоносный Агент будет виден визуально. Также видно наличие функции eval(), которую агенты содержать не должны:



3. Проверить наличие файлов журнала keylogger «.sess», «.idSess», «.session».
Пример команды для поиска:

```
find / -name '.sess' -o -name '.idSess' -o -name '.session'
```

Наличие любого из этих файлов подтверждает факт установки keylogger. На текущий момент известный способ установки: модификация файла панели управления CMS 1C Bitrix (/bitrix/admin/index.php). В начало файла дописывается вызов функции "file_put_contents(..., print_r($_REQUEST,1))". В результате в файл "/bitrix/tools/.sess" записываются все попытки аутентификации (в том числе логин, пароль и session cookie). Дополнительная опасность в том, что в журнал keylogger могут записываться также session cookie для других веб-приложений, существующих на том же домене, что и скомпрометированная CMS 1C Bitrix. В таком случае злоумышленник получает доступ не только к административной панели Bitrix, но и валидную сессию для других веб-приложений.

4. Проверить иные способы закрепления доступа на узле.
Карта с описанием типовых способов закрепления в ОС Linux:
https://pberba.github.io/assets/posts/common/20220201-linux-persistence.pdf
Цикл статей, описывающих поиск техник закрепления, отраженных на карте:
https://pberba.github.io/security/

4.2 Сдерживание

В случае, если нет возможности обновить CMS до актуальной версии, можно заблокировать POST-запросы к уязвимым файлам.

4.2.1 Модификация файлов WEB-приложения

Для каждого сайта необходимо модифицировать следующие 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 функцией «require_once» добавить следующий код:

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

4.2.2 Ограничение доступа к уязвимым файлам средствами WEB-сервера

Добавить в конфигурацию WEB-сервера запрещающие правила.

Пример правил для NGINX:

```
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;
        }
}
```

4.2.3 Ограничение доступа к уязвимым файлам средствами WAF/NGFW

Запретить прямые обращения POST-запросами к файлам:

/bitrix/tools/html_editor_action.php

/bitrix/tools/vote/uf.php

5 Очистка зараженного узла и восстановление приложения

1. Остановить службу WEB-сервера.
2. Проверить наличие иного работающего в памяти процесса, исполняющего PHP, и остановить этот процесс.

```
kill $(ps aux | grep 'php' | awk '{print $2}')
```

3. Очистить cache WEB-приложения.
4. Удалить выявленные ранее сторонние вредоносные файлы (п. 4.1.1, п. 4.1.3, п 4.1.5).
5. Проверить резервную копию сайта аналогично п. 4.1.1, п. 4.1.3, п. 4.1.4, п. 4.1.5.

В случае обнаружения вредоносных объектов требуется удалить вредоносные объекты или имплементации вредоносного кода.

Дополнительно рекомендуется использовать механизм контроля целостности файлов.

(https://dev.1c-bitrix.ru/user_help/settings/security/security_file_verifier.php)

6. Восстановить сайт из резервной копии.
7. Проверить работоспособность всех разделов сайта.
8. Обновить «1С-Битрикс: Управление сайтом» и PHP до актуальных версий.
9. Сменить пароли всех учетных записей CMS.
10. Изменить ключ БД "signer_default_key”.

```
$oldKey = \Bitrix\Main\Config\Option::get('main', 'signer_default_key', false);
\Bitrix\Main\Config\Option::set('main', 'signer_default_key', hash('sha512', uniqid(rand(), true)));
echo "OldKey was: $oldKey\n";
```

6 Рекомендации по защите WEB-приложения

- Перевести сайт на актуальную версию PHP 8. Инструкция.
- Обновить «1С-Битрикс: Управление сайтом» до актуальных версий.
- Установить, включить и настроить согласно рекомендациям модули:
  - «Проактивный фильтр (Web Application Firewall)»
  - «Контроль активности»
- Выполнить проверку WEB-приложения средствами «Сканер безопасности»
- Закрыть доступ к файлам на уровне сервера (например, в .htaccess):
  - /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.p
- Ограничить доступ к панели управления CMS из сети Интернет (оставить доступ только для IP из ЛВС, опционально расширить список легитимными публичными IP) или настроить аутентификацию по OTP.
- Включить логирование событий доступа к WEB-приложению (все типы запросов) и ошибок (error.log).

7 Восстановление работоспособности в случае блокировки

По данным открытых источников, в некоторых случаях сайт может быть заблокирован Национальным координационным центром по компьютерным инцидентам (НКЦКИ) по причине его взлома с последующим размещением противоправного контента и использованием злоумышленниками для проведения компьютерных атак на критическую информационную инфраструктуру Российской Федерации в соответствии со статьей 5 Федерального закона № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», пунктом 5.1 Приказа ФСБ России от 24.07.2018 г. № 366 и пунктом 9 Правил централизованного управления сетью связи общего пользования, утвержденных постановлением Правительства Российской Федерации от 12 февраля 2020 года № 127.

Блокировка применяется до момента фиксации НКЦКИ факта удаления противоправного контента.

В таком случае, после устранения дефейса, бэкдора и уязвимостей свяжитесь с командой НКЦКИ.

107031, г. Москва, ул. Большая Лубянка, д. 1/3
Email: incident@cert.gov.ru
Сайт: http://cert.gov.ru/
Тел.: +7 (916) 901-07-42

8 Контакты

«СайберОК» — энергичный стартап, созданный ветеранами кибербезопасности, выходцами из Positive Technologies и Лаборатории Касперского. Мы разрабатываем передовую платформу кибербезопасности на базе технологий с открытым исходным кодом, занимаемся пентестами и расследованием инцидентов.

АО Сайбер ОК
123112, г. Москва, Пресненская набережная, д.12
+7 (495) 137-7337
https://www.cyberok.ru/
info@cyberok.ru