Обновись сейчас! ТОП-5 самых опасных уязвимостей сентября

В этой заметке расскажем о самых опасных уязвимостях сетевого периметра, которые мы в CyberOK отслеживали в сентябре 2023 года. Сегодня в топ-5:

- Гонки на Битриксе (BDU:2023-05857);
- Экспериментальный разгласитель почты (ZDI-23-1473 и их друзья);
- Когда Пойнт слишком Шеринг (CVE-2023–29357);
- Не звоните наверх (CVE-2022-46764);
- Город Команд (CVE-2023-42793).

1. Гонки на Битриксе

Состояние гонок в модуле Landing в CMS 1С-Битрикс приводящее к выполнению произвольного кода (BDU:2023-05857).

Система управление сайтом 1С-Битрикс постоянно находится в фокусе злоумышленников. Массовые взломы сайтов различных организаций проходят волнами уже не первый год. Прошлые уязвимости CVE-2022-27228 («Опросы, голосования»/«Vote» и «Визуальный редактор»/”html_editor_action”) активно эксплуатируются злодеями с марта 2022 года и конца-края не видно.

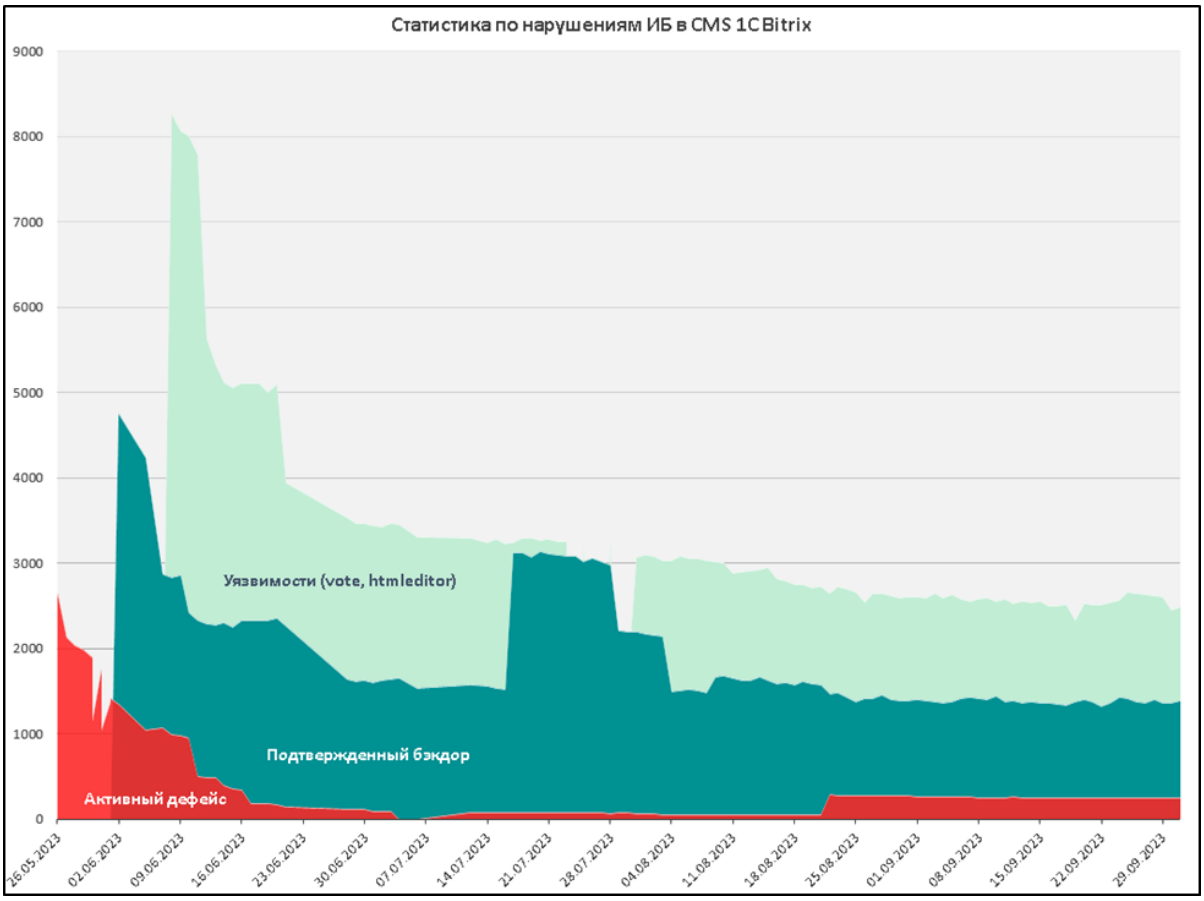
Новая уязвимость в модуле Конструктора сайтов (Landing) встречается во всех версиях вплоть до 23.800.0 и исправлена в версии 23.850.0. Шум поднялся 21.09.2023 после публикации уведомления БДУ ФСТЭК.
Разработчик выпустил обновление заранее, 14 сентября 2023, с пометкой «Критическое обновление безопасности. Рекомендуется к немедленной установке». Команда СайберОК присоединяется к рекомендации: **обновить прямо сейчас!!!**

Важно! В CMS 1С-Битрикс модули имеют собственное версионирование, отличное от модуля ядра, поэтому после обновления надо проверить, что версия именно модуля Landing не ниже v23.850.0. Да и ядро неплохо бы обновить.

Сейчас СКИПА видит на своих радарах около 160,000 сайтов подверженных этой уязвимости, при этом динамика установки обновлений очень небольшая (см. график).

Эксплойт пока не публичен, флоу эксплуатации достаточно заморочен и по-своему красив. Этакая гоночная многоходовочка. Чем-то напомнил цепочку багов в Microsoft SharePoint, о которой ниже. Спасибо тем, кто находит (и патчит) такие интересные баги. Остается только скрестить пальцы и надеяться, что эксплойт не утечет в паблик до того, как большинство обновится.

При обновлении было бы полезно еще раз проверить свои сайты на признаки компрометации, изложенные в нашем документе. Практика показывает, что взломанный сайт может «нормально» работать месяцами и попутно делиться паролями и персональными данными со злоумышленниками до тех пор, пока они не решат, что он бесполезен и «сломают» его окончательно. Ну или подерутся там, решая чья это «корова». Бывает.
В настоящее время СайберОК СКИПА отслеживает более 2300 сайтов с уязвимостью Vote и около 300 с «Визуальный редактор». 1500 из них взломаны злоумышленниками и имеют внешние признаки компрометации.



P.S. Еще пару слов о битрогенезисе.

На конференции Kazhackstan Антон Лопаницын aka Bo0oM в своем докладе «Выйди и зайди нормально!» рассказал о некоторых особенностях административного интерфейса CMS 1С-Битрикс. Не то чтобы ужас-ужас, но доступ к /bitrix/admin/* из внешних сетей рекомендуем ограничить. Можно и просто по IP. Мало ли что...

Ссылки:
https://dev.1c-bitrix.ru/community/forums/messages/forum6/topic147346/message731384/#message731384
https://bdu.fstec.ru/vul/2023-05857
https://www.cyberok.ru/skipa.html
https://www.cyberok.ru/docs/CyberOK-bitrix_web_14.pdf
https://coollib.net/b/669667-anton-lopanitsyn-vyiydi-i-zaydi-normalno/download
https://dev.1c-bitrix.ru/docs/versions.php?lang=ru&module=landing
https://www.bitrix24.ru/features/box/box-versions.php?module=landing
https://www.bitrix24.com/features/box/box-versions.php
https://safe-surf.ru/upload/VULN-new/VULN.2023-09-21.1.pdf

2. Эксперименты с разглашением почты

Удаленное выполнение кода в Exim не требующее аутентификации.

27 сентября ZDI опубликовала информацию о нескольких 0-day уязвимостях в популярном почтовом сервере Exim. Памятуя массовые взломы Exim в 2019 году мы почувствовали легкое беспокойство, переходящее в панику. Дело в том, что на момент публикации баги не были закрыты, обновление отсутствовало. Что делать — непонятно.
Немного поругавшись с ZDI в рассылке Open Wall oss-sec, разработчики выпустили обновления для наиболее критичных уязвимостей.

Как пишет Хайко Шлиттерманн (Heiko Schlittermann):

- 3 из них связаны с SPA/NTLM и EXTERNAL аутентификацией. Если вы не используете SPA/NTLM или EXTERNAL аутентификацию, на вас это не влияет.
- Одна проблема связана с данными, полученными от прокси-сервера прокси-протокола. Если вы не используете прокси перед Exim, на вас это не влияет. Если ваш прокси заслуживает доверия, вы не пострадаете.
- Один связан с libspf2. Если вы не используете тип поиска `spf` или условие `spf` ACL, на вас это не влияет.
- Последний связан с поиском DNS. Если вы используете надежный сервер (который проверяет полученные данные), вы не затронуты.

Версии с устранением CVE-2023-42115 и сестер на 3 октября 2023 года: 4.97_RC1-2, 4.94.2-7 и 4.96-15. Эксплойт пока не публичен, но ходят слухи о точечных взломах Exim, что вселяет беспокойство и желание **обновить прямо сейчас!** Рейтинг EPSS 0.975 – очень высокий, что совпадает с нашим ощущением. По последним данным от разработчиков, наиболее критичные уязвимости могут использоваться только в случаях специфических конфигураций (например, аутентификации NTLM, SPA, EXTERNAL) или в случае, если ваш DNS-сервер не верифицирует DNS-ответы. Это должно снизить поверхность атаки. Осталось только понять, что именно DNS-сервер должен считать подозрительным и отбрасывать как негодное… Задачное пока.

Мы отслеживаем в Рунете более 56 тысяч (!) Exim уязвимых версий. При этом многие сервисы уязвимы и для более старых критичных уязвимостей. Приведем статистику по версиям Exim в Рунете:

Версия	%
Exim 4.96	18,18
Exim 4.93	15,87
Exim 4.94.2	12,08
Exim 4.90_1	11,61
Exim 4.92	9,13
Exim 4.95	7,45
Exim 4.89	4,80
Exim 4.86_2	4,80
Exim 4.92.3	4,00
Exim 4.94	3,85

Из этих десятков тысяч потенциальных мишеней большая доля (~91%) развернуты на площадках хостеров. Более того, у некоторых заботливых хостеров на новой VPS Exim уже установлен и служба добавлена в автозапуск. У правильно заботливых хостеров она привязана к localhost, что радует.

Коллеги из хостинг-провайдеров, обратите внимание или свяжитесь с нами, если нужна дополнительная информация.

```
e6e6e@ok-      1:~$ netstat -tulpn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 ::1:25                  :::*                    LISTEN      -
e6e6e@ok-      :~$ systemctl status exim4
● exim4.service - LSB: exim Mail Transport Agent
     Loaded: loaded (/etc/init.d/exim4; generated)
     Active: active (running) since Tue 2023-10-03 11:59:28 MSK; 5min ago
       Docs: man:systemd-sysv-generator(8)
    Process: 601 ExecStart=/etc/init.d/exim4 start (code=exited, status=0/SUCCESS)
      Tasks: 1 (limit: 4692)
     Memory: 18.9M
        CPU: 360ms
     CGroup: /system.slice/exim4.service
             └─874 /usr/sbin/exim4 -bd -q30m
```

Примечателен таймлайн уязвимости. Процитируем разработчиков:
«ZDI связался с нами в июне 2022 года. Мы спросили подробности, но не получили ответы, с которыми мы смогли работать. Следующий контакт с ZDI состоялся в мае 2023 года… Остальные проблемы являются спорными или не содержат информации, которая необходима для их исправления… Мы более чем рады предоставить исправления для всех проблем, как только мы сможем получить подробную информацию».

Т.е. дырка была известна ZDI больше года, но «лежала на полочке» (нет) без передачи детальной информации разработчику. Очень радует «скоординированное разглашение» ZDI без выпуска обновления производителей. У нас есть такие эксплойты, но мы вам о них не расскажем. Координированная такая координация.

PS. Что-то этих идентификаторов стало так много, сами запутались. На всякий случай приведем табличку со статусом (под катом).

```
ZDI-23-1468 | ZDI-CAN-17433 | CVE-2023-42114 | Exim bug 3001
-------------------------------------------------------------
Subject:    NTLM Challenge Out-Of-Bounds Read
CVSS Score: 3.7
Mitigation: Do not use SPA (NTLM) authentication
Subsystem:  SPA auth
Fixed:      04107e98d, 4.96.1, 4.97

ZDI-23-1469 | ZDI-CAN-17434 | CVE-2023-42115 | Exim bug 2999
-------------------------------------------------------------
Subject:    AUTH Out-Of-Bounds Write
```

```
CVSS Score: 9.8
Mitigation: Do not offer EXTERNAL authentication.
Subsystem:  EXTERNAL auth
Fixed:      7bb5bc2c6, 4.96.1, 4.97

ZDI-23-1470 | ZDI-CAN-17515 | CVE-2023-42116 | Exim bug 3000
------------------------------------------------------------
Subject:    SMTP Challenge Stack-based Buffer Overflow
CVSS Score: 8.1
Mitigation: Do not use SPA (NTLM) authentication
Subsystem:  SPA auth
Fixed:      e17b8b0f1, 4.96.1, 4.97

ZDI-23-1471 | ZDI-CAN-17554 | CVE-2023-42117 | Exim Bug 3031
------------------------------------------------------------
Subject:    Improper Neutralization of Special Elements
CVSS Score: 8.1
Mitigation: Do not use Exim behind an untrusted proxy-protocol proxy
Subsystem:  proxy protocol (not socks!)
Fix:        not yet

ZDI-23-1472 | ZDI-CAN-17578 | CVE-2023-42118 | Exim Bug 3032
------------------------------------------------------------
Subject:    libspf2 Integer Underflow
CVSS Score: 7.5
Mitigation: Do not use the `spf` condition in your ACL
Subsystem:  spf
Remark:     It is debatable if this should be filed against
            libspf2.

ZDI-23-1473 | ZDI-CAN-17643 | CVE-2023-42219 | Exim Bug 3033
------------------------------------------------------------
Subject:    dnsdb Out-Of-Bounds Read
CVSS Score: 3.1
Mitigation: Use a trustworthy DNS resolver which is able to
            validate the data according to the DNS record types.
Subsystem:  dns lookups
Fix:        not yet
Remark:     It is still under consideration.
```

Ссылки:

https://www.zerodayinitiative.com/advisories/ZDI-23-1469/

https://www.opennet.ru/opennews/art.shtml?num=50870

https://seclists.org/oss-sec/2023/q3/259

https://tracker.debian.org/news/1467882/accepted-exim4-497rc1-2-source-into-unstable/

https://www.openwall.com/lists/oss-security/2023/09/29/3

3. Точка разглашения

Удаленное выполнение кода в Microsoft SharePoint не требующее аутентификации.

Критическими уязвимостями в продуктах Microsoft никого не удивить. Начиная с MS01-033 (или раньше? кто помнит, пишите в комменты), они десятки раз становились причинами масштабных взломов и эпидемий сетевых червей. Продукт Microsoft Sharepoint далеко не первый в этом печальном рейтинге, но...

Баги CVE-2023–29357 & CVE-2023–24955 были использованы 22 марта 2023 на конкурсе Pwn2Own Vancouver 2023, чтобы получить приятный баунти, и закрыты Microsoft в KB5002390 в мае того же года.

Обстановка накалилась, когда ребята из Starlabs 25 сентября опубликовали детальный технический райтап описывающий флоу экплуатации, после которого даже школьнику стало понятно как сделать экплотес, а стало быть и шелкодес. Любители эксплойтостроительства не подвели и уже через пару дней весь гит был забит разной злобы нуклейками и питончиками. Кто-то даже на C# эксплойт написал. Говорят, что ChatGPT заставил. Где мой тинфоилхэт?..

Нельзя ждать, обновитесь прямо сейчас!

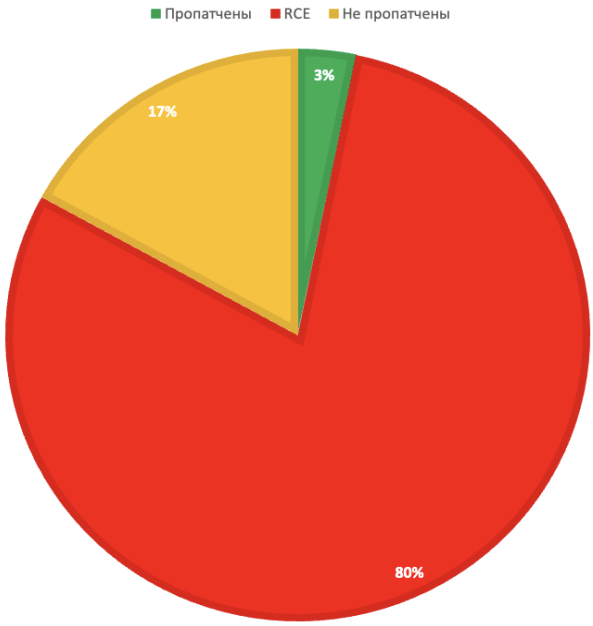
В настоящее время мы отслеживаем более 2500 подключенных к Интернет SharePoint глобально из них около 650 в Рунете (ухх, спокойнее).

Немного «подката» для любителей статистики.

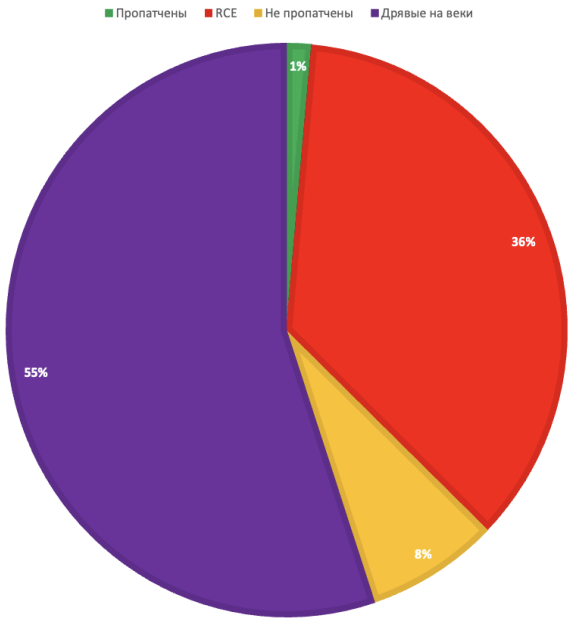
Вот так выглядит топ актуальных версий SharePoint по миру.

15.0.0.4849	38.07%
16.0.0.4705	35.93%
15.0.0.4569	18.51%
16.0.0.10396	7.59%
16.0.0.10337	7.40%
16.0.0.10401	6.06%
15.0.0.4420	4.82%
14.0.0.4762	4.77%
16.0.0.5403	4.53%

Красиво, но непонятно. Но если разметить «неуязвимые», «дырявые» и «прям бери и ломай», то 80% хакабельно без особых усилий.



И это если брать только поддерживаемую версию SharePoint 2019 и 2016. Если добавить более ранние версии, такие как SharePoint 2013 и старше, получаем совсем печальную картинку.



Остается только предполагать, сколько эта бага будет жить во внутренних сетях и приносить приятные пробивы пентестерам и вкусные битки рансомварщикам.

Ссылки:
https://www.zerodayinitiative.com/blog/2023/3/21/pwn2own-vancouver-schedule-2023
https://starlabs.sg/blog/2023/09-sharepoint-pre-auth-rce-chain/
https://github.com/LuemmelSec/CVE-2023-29357
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29357
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24955

4. Не звоните наверх

Выполнение кода в TrueConf до аутентификации.

Печально, но админы и девопсы не любят патчить не только продукцию Microsoft. Связка из двух уязвимостей в API аутентификации (CVE-2022-46764) и в реализации хранимых в PostgreSQL функций (CVE-2022-46763) позволяла неавторизованному злоумышленнику выполнить произвольный код на сервере TrueConf Server. Ну как «позволяла» — уязвимость, выявленная ребятами из Solidlab, широко известна с 20 декабря 2022 года, производитель исправил ее в версии 5.2.6, выпущенной 28 ноября 2022), общедоступного эксплойта нет. Но те, кто занимаются расследованием инцидентов знают то, что знают. И говорят хором: **обновитесь прямо сейчас!**

Ссылки:
https://solidlab.ru/our-news/145-trueconf.html
https://trueconf.ru/products/changelog.html#server-5-2-6
https://nvd.nist.gov/vuln/detail/CVE-2022-46763
https://nvd.nist.gov/vuln/detail/CVE-2022-46764

5. Город Команд

Удаленное выполнение кода в JetBrains TeamCity до аутентификации.

Уязвимость CVE-2023-42793 могла бы пройти тихо и незаметно. Ну подумаешь, yet another dev tool RCE? Мало ли их было и будет в этих ваших GitLab, Confluence и прочих Jira?

И патч вышел вовремя, и информация о проблеме подробная. Слишком подробная, к сожалению...

В вышедшем 21 сентября 2023 уведомлении содержится много полезной информации. Без сарказма. Респект AppSec команде JetBrains, очень информативный и полезный сайт, подробные адвизки и все такое. Но в тексте упоминаются «Security patch plugin», скачав которые любой скажет...

```
46    for (String path : myMatchingPathsValue) {
47      if (path.equals("/**/RPC2"))
48        toRemove.add(path);
      }
51    myMatchingPathsValue.removeAll(toRemove);
53    Loggers.SERVER.debug("Applying a fix for CVE-2023-42793: n
55    Loggers.SERVER.info("Fix for CVE-2023-42793 has been succe
56  } catch (Throwable e) {
57    Loggers.SERVER.warnAndDebugDetails("Failed to apply a fix
    }
```

А что, так можно было? Ну или что сказали бы вы?

Ну и буквально через несколько дней в сети появились вполне себе рабочие эксплойты, некоторые из которых даже не надо дорабатывать напильником. А после того, как 27 сентября был опубликован технический разбор, начался чад кутежа, огонь индикаторов компрометации и прекрасное будущее. Что значит (хором): **обновись прямо сейчас!**

Интересно, что 28 сентября TeamCity опубликовали подробный таймлайн. Только приписка «Post-Mortem» немного смущает. Они знают тоже самое, что и те, кто занимается расследованием инцидентов?

Ссылки:

https://blog.jetbrains.com/teamcity/2023/09/critical-security-issue-affecting-teamcity-on-premises-update-to-2023-05-4-now/

https://www.jetbrains.com/privacy-security/issues-fixed/

https://www.sonarsource.com/blog/teamcity-vulnerability/

https://blog.jetbrains.com/teamcity/2023/09/cve-2023-42793-vulnerability-post-mortem/

https://nvd.nist.gov/vuln/detail/CVE-2023-42793

Откуда мы все это знаем?

Мы в СайберОК разрабатываем Систему Контроля и Информирования о Поверхности Атак (СКИПА), перелопачивающую сотни гигабит трафика в сети и петабайты данных в хранилке, чтобы выявлять актуальные угрозы и вовремя защищать компании и организации. Да, это как Shodan, Censys, MaxPatrol или RiskIQ, только лучше!
СКИПА уже доступна для корпоративных клиентов и, надеемся, в скором времени мы откроем доступ независимым экспертам и баг хантерам.
Хотите больше узнать про управление поверхностью атак и защитить свой периметр? Пишите нам, заходите в телегу, присоединяйтесь к команде!
Мы всегда ищем крутых разработчиков (golang), экспертов в области кибербеза, пентестеров.

До новых встреч и **обновись сейчас!**