www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

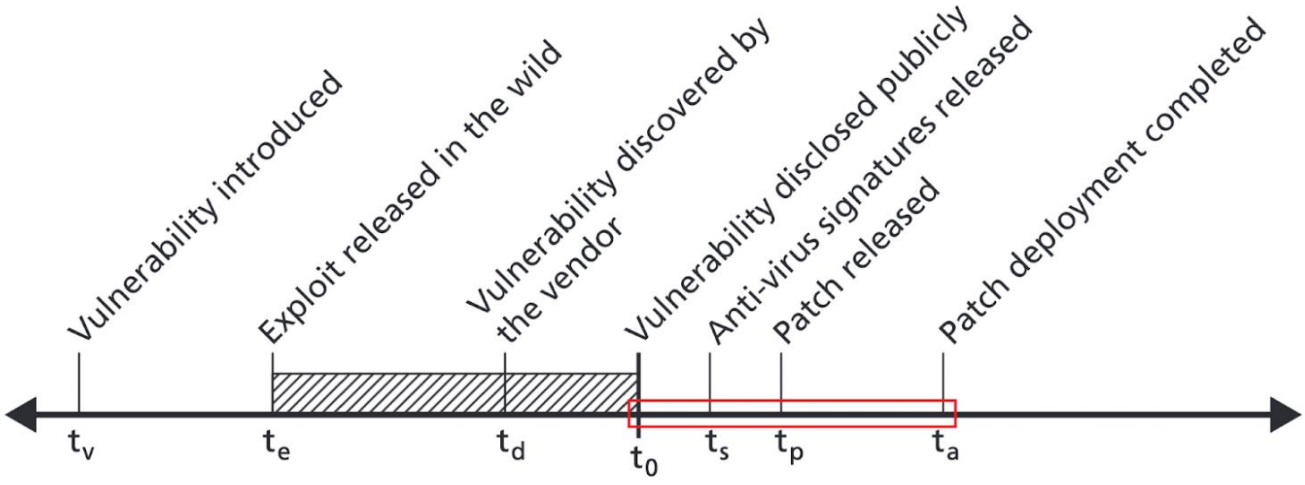
А был ли патчик? Как долго живут уязвимости в Рунете

Максим Пушкин – старший специалист
направления развития экспертизы

Меня зовут Максим Пушкин, я работаю в компании СайберОК. Если вы что-то слышали о нас, то знаете, что последние 3 года мы разрабатываем систему СКИПА (Система Контроля и Информирования о Поверхности Атак).

В ходе этой работы мы с интересом изучаем сервисы, находящиеся в Интернете, и рассматриваем их также с точки зрения безопасности.

В этой статье речь пойдет о простом вопросе: сколько дней/недель/месяцев в среднем живёт уязвимость в реальной жизни?



Жизненный цикл уязвимости

Если рассматривать обобщенный жизненный цикл уязвимости, то можно выделить несколько ключевых точек:

1. Первая эксплуатация уязвимости.
2. Получение вендором информации об уязвимости.
3. Появление информации об уязвимости в публичных источниках.

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

4. Выпуск вендором патча, устраняющего уязвимость.
5. Конечный этап жизненного цикла уязвимости — установка патча на сам уязвимый сервис.

Среди них, нас интересует последние две, а если точнее — расстояние между ними, то есть то время, которое уходит у администраторов и владельцев сетевых ресурсов на то, чтобы установить патч на свой сервис.

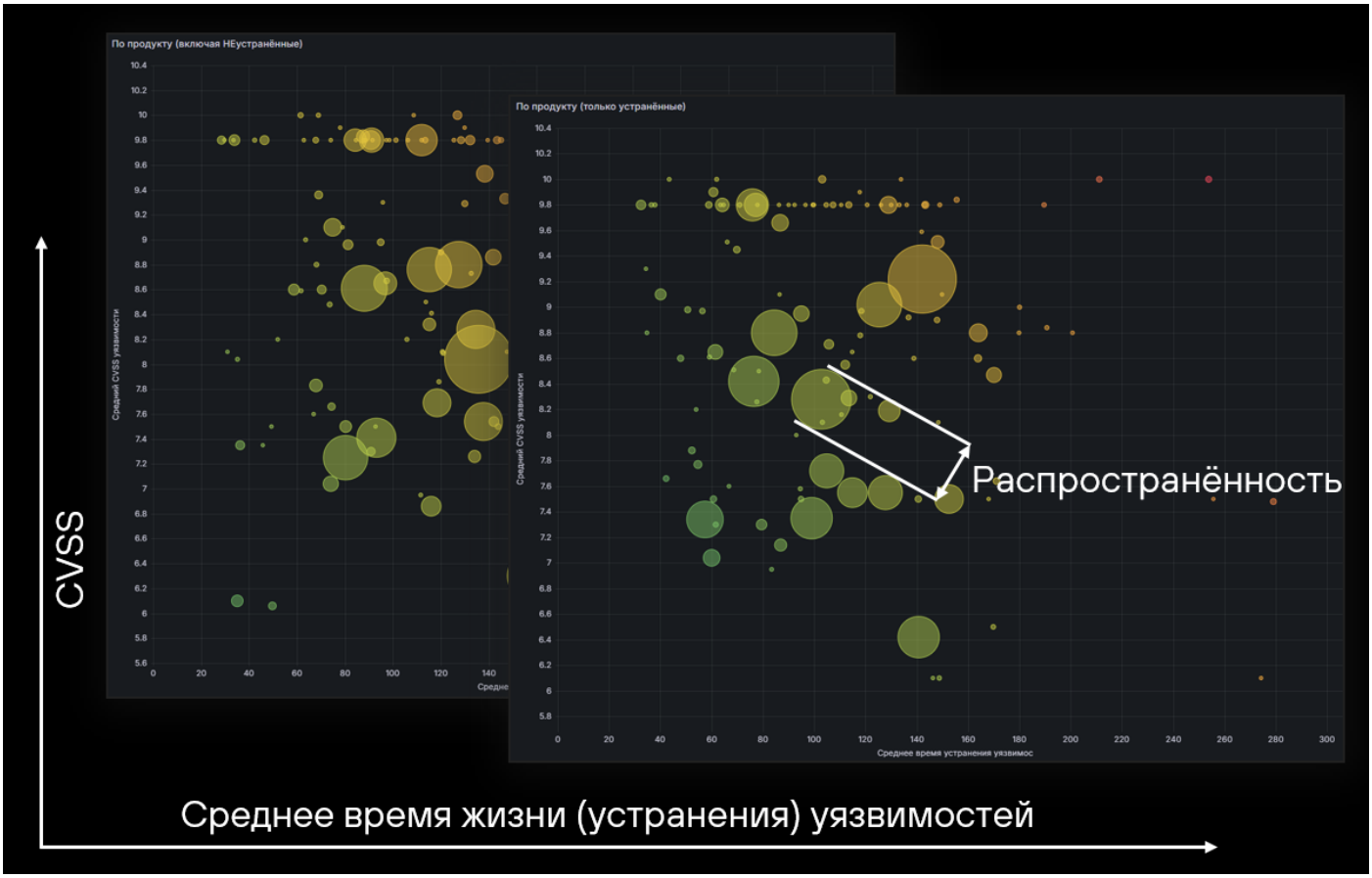
Именно это мы решили посчитать с помощью данных, накопленных нашей системой за годы регулярного мониторинга Рунета.

Методология

При подсчетах использовались две метрики:

1. Время устранения уязвимости. Данная метрика используется в тех случаях, когда сервис был уязвим на протяжении какого-то времени, спустя которое, уязвимость на нём пропала.
2. Среднее время жизни уязвимости. Данная метрика более широкая, чем предыдущая и включает в себя и те случаи, когда уязвимость на момент последней проверки всё ещё доступна.

После сбора результатов мы приступили к визуализации.



Визуализация результатов

На получившейся пузырьковой диаграмме, каждый круг представляет из себя вендора или продукт, для которого рассчитаны такие параметры, как:

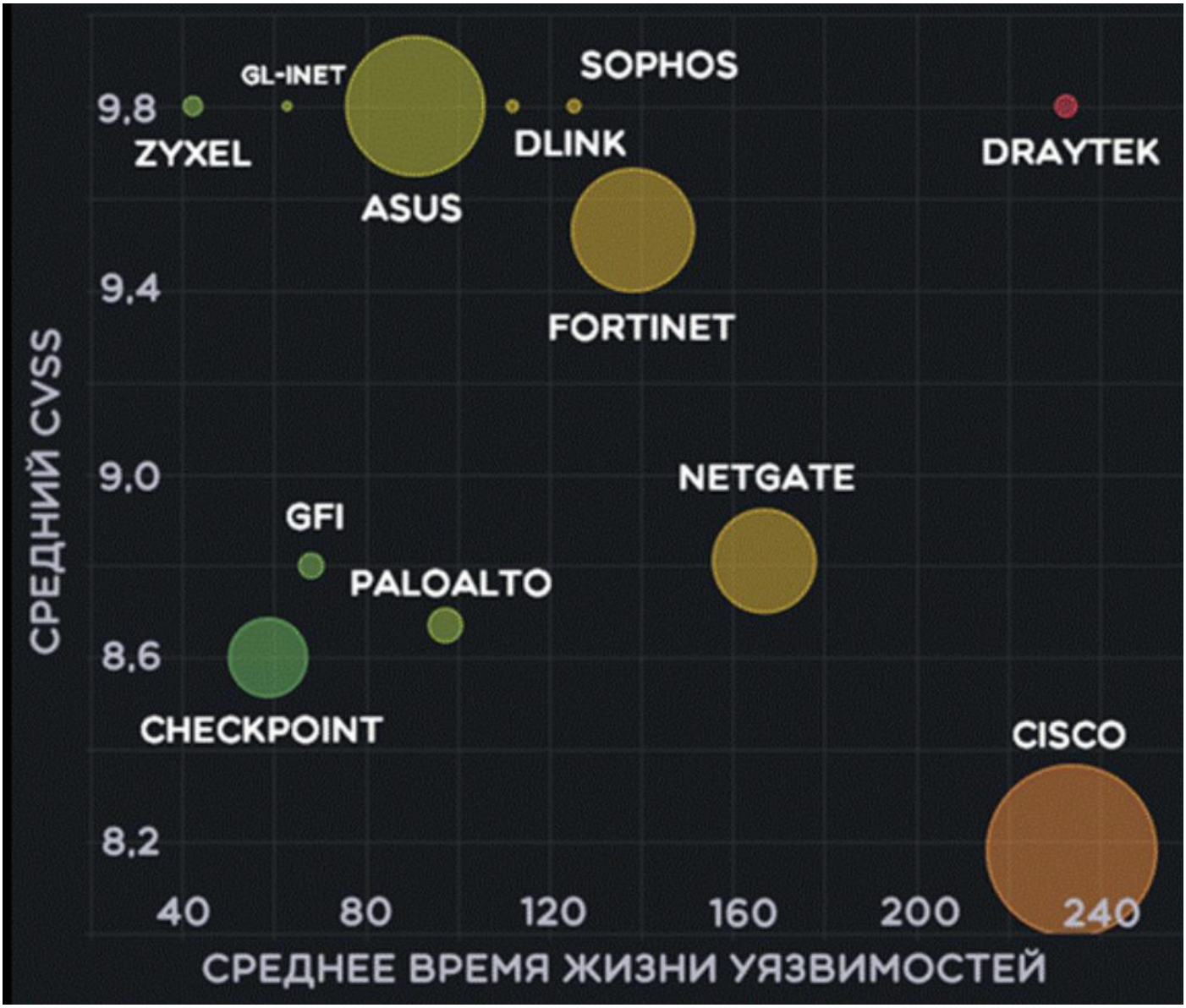
- среднее время жизни (устранения) уязвимостей (ось X);
- средний рейтинг критичности уязвимостей (CVSS) (ось Y);
- распространенность уязвимости (диаметр круга).

После того, как данные по более чем 100 продуктам (всего в статистике насчитывается 133 продукта, а общее число уязвимостей составляет 400) отобразились на одной такой диаграмме, стало ясно, что прочитать её и сделать какие-то выводы — задачка со звездочкой. Поэтому далее будут рассмотрены самые интересные категории продуктов, а итоговый список всех продуктов опубликован на сайте CyberOK.

NGFW и сетевое оборудование

Продукты данной категории специфичны тем, что их интерфейсы управления не должны быть доступны из Интернета в принципе. Но они доступны, и не в малом количестве. И при этом обновляются достаточно редко для таких критичных систем.

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337



NGFW и сетевое оборудование

В таблице ниже представлены точные значения для продуктов из данной категории.

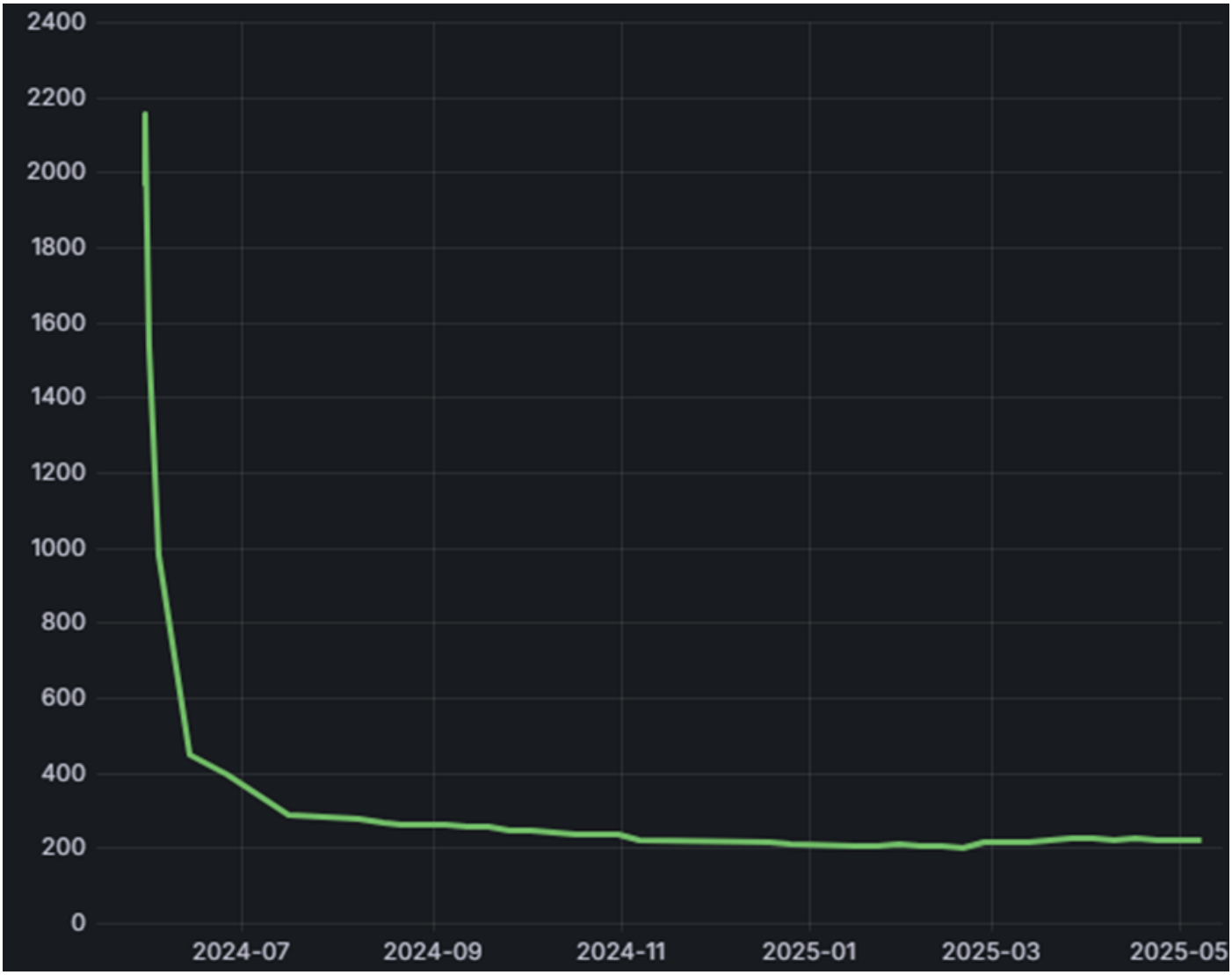
Вендор	Продукт	Количество уязвимых продуктов на сегодня, тыс.	Время жизни, дни
Cisco	ASA	3.2	235
Cisco	IOS-XR, SmallBusiness	0.1	162

Fortinet	FortiOS, Fortimanager	1.9	138
Checkpoint	Security Gateway	2.1 → 0.2	58
Paloalto	Pan-OS	0.8 → 0.1	97
Netgate	Pfsense	2.0	167
Asus	Routers	2.5 → 0.5	90
Draytek	Vigor	0.05	233
Sophos	SFOS	0.01	200
Zyxel	NAS	0.1	42
GL.iNet	Routers	0.02	62.9
Dlink	Routers	0.03	112
GFI	KerioControl	0.2	68

Так, среднее время жизни уязвимости одного из популярных продуктов Cisco ASA составляет около 8 месяцев. По остальным продуктам — 3–5 месяцев. Однако есть и исключения — для некоторых продуктов, в ходе наблюдений, количество уязвимых сервисов существенно сократилось. Для таких в таблице представлены два числа: первое — сколько уязвимых сервисов мы обнаружили на начало наблюдений, второе — сколько мы обнаруживаем сейчас.

Одним из таких примеров является Check Point.

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

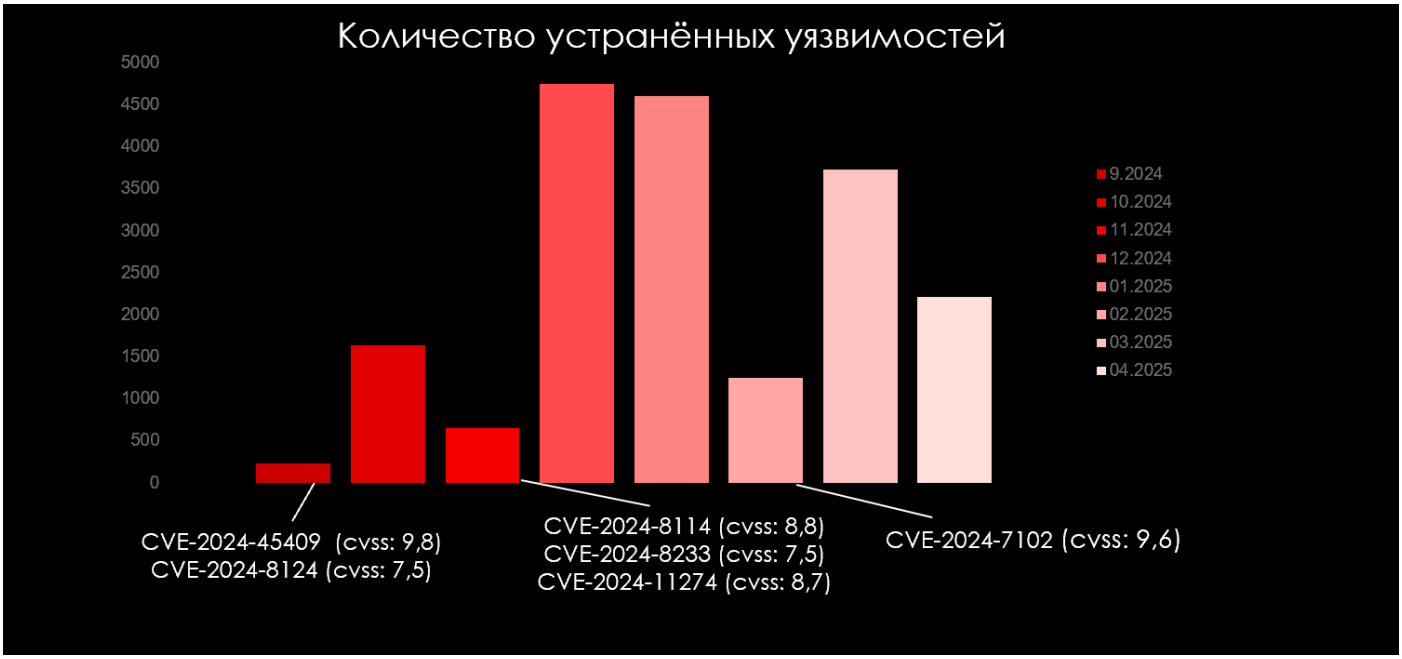


Количество обнаруживаемых уязвимых сервисов

В мае прошлого года появилась уязвимость, которая позволяла злоумышленнику выполнить чтение произвольного файла. После того, как в сообществе поднялась шумиха (в том числе, появились данные о распространенности этой уязвимости), количество уязвимых инстансов на следующий день упало на 25%, через неделю — вдвое, а через месяц — на 75%. В дальнейшем значение стабилизировалось, и около 200 уязвимых Check Point до сих пор подвержены данной уязвимости.

Этот пример является показательным с точки зрения этичности публикации данных об уязвимостях — это работает, и действительно побуждает администраторов обновлять свои ресурсы, делая их безопаснее.

Другим примером на котором можно наглядно увидеть динамику устранения уязвимостей является GitLab.



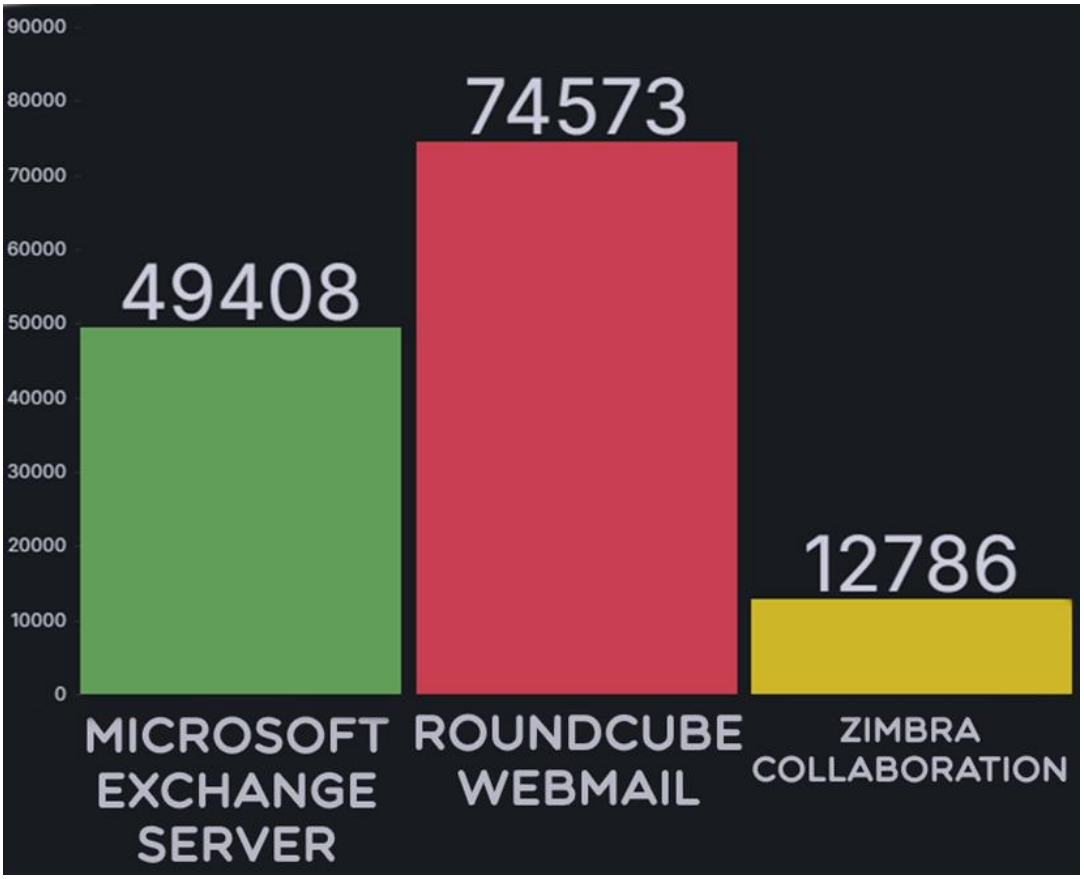
Количество устраненных уязвимостей в GitLab по месяцам

На данной диаграмме представлено количество устраненных уязвимостей по месяцам за 8 месяцев (сент. 2024 — апр. 2025). Можно заметить, что некоторые администраторы следят за инфополем: каждый всплеск устранений совпадает с появлением одной или нескольких новых критичных уязвимостей в предыдущем месяце.

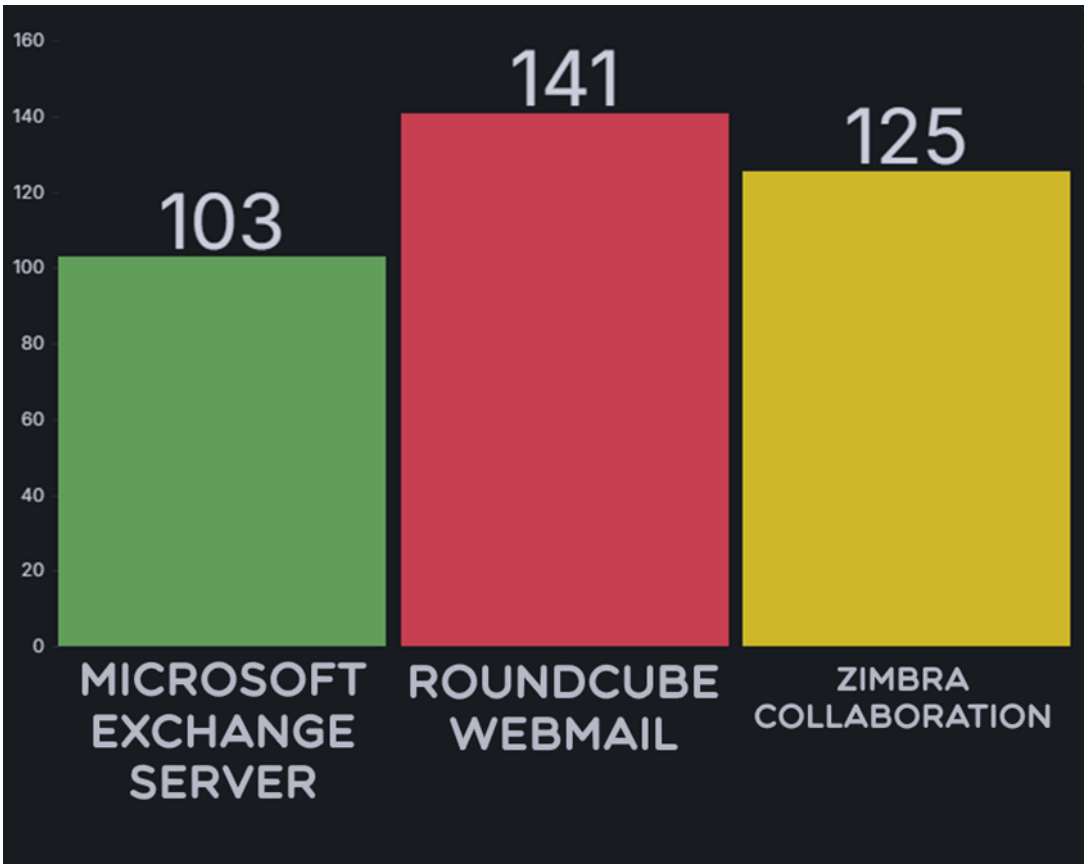
Почтовые системы

Следующая категория продуктов — это почтовые системы.

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337



Распространенность ПО



Среднее время устранения уязвимостей

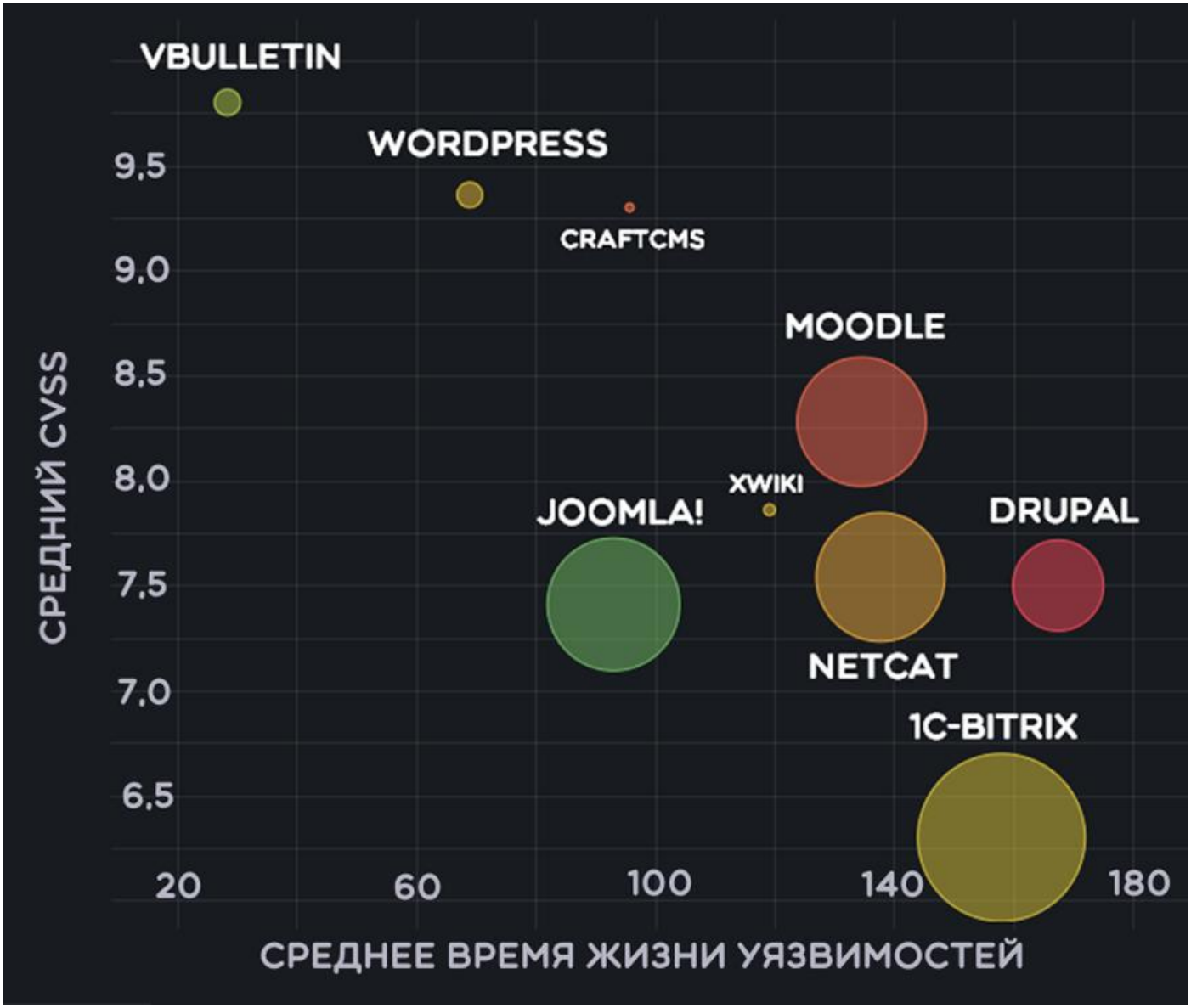
www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Удивительный факт: на радарах СКИПА мы обнаруживаем около 50 тысяч Microsoft Exchange Server. И это несмотря на то, что Microsoft давно ушёл с российского рынка. До сих пор эта почтовая система является одной из самых популярных, и, более того, уязвимости в ней в России устраняются быстрее, чем у аналогичных продуктов других вендоров.

Отсюда можно сделать вывод — такой крупный вендор, как Microsoft, следит за своей безопасностью, регулярно публикует патчи и уведомляет своих пользователей о наличии и появлении той или иной уязвимости, что менее свойственно даже популярным Open-Source решениям.

CMS-системы

Данная категория характеризуется наиболее популярными и распространёнными продуктами, в которых также встречаются критичные уязвимости.



Среднее время жизни уязвимостей в ПО класса CMS

Если мы посмотрим на диаграмму, то увидим, что среднее время жизни уязвимостей в таких продуктах находится в районе 3 месяцев или даже больше. При этом количество уязвимых сервисов может переваливать за десятки тысяч.

Самое популярное ПО

Если посмотреть на самые популярные в Рунете продукты, то можно увидеть, что в среднем им не свойственно быстрое устранение уязвимостей.

Среднее время устранения уязвимостей самого популярного ПО

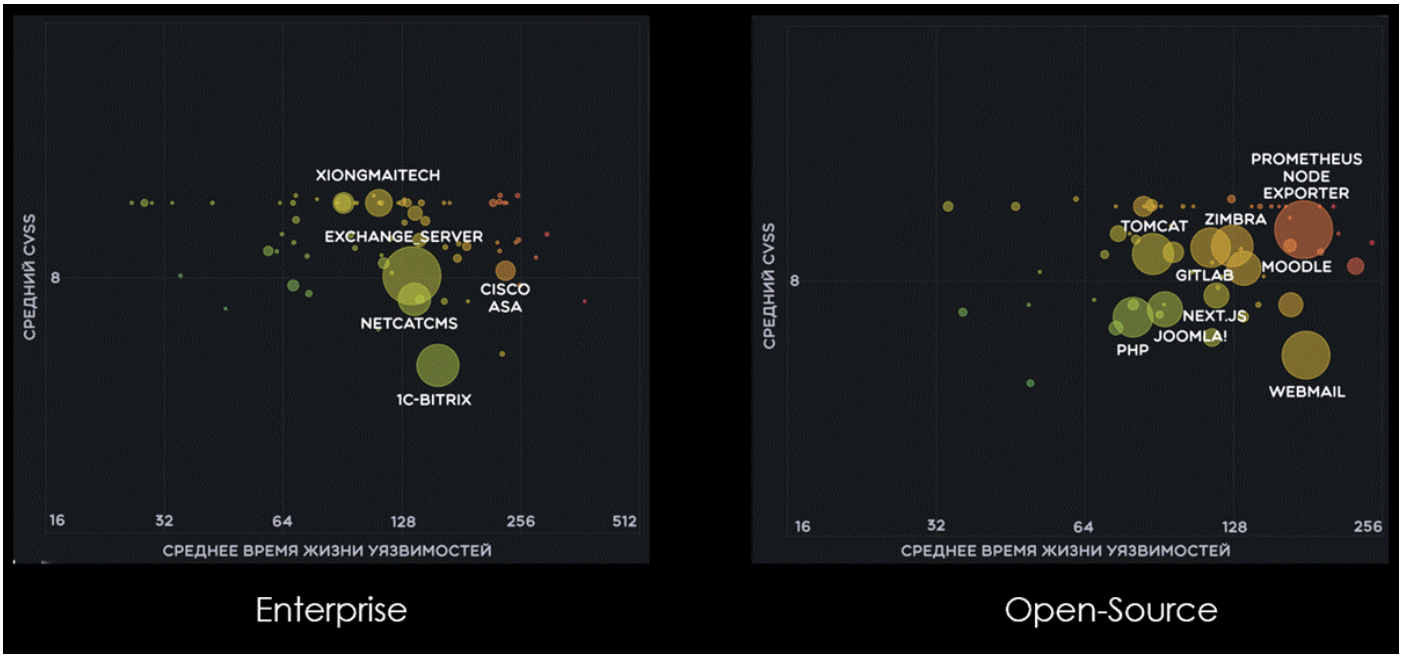
На диаграмме представлены те продукты, для которых наблюдаемое количество **уязвимых** сервисов превышает 10 тысяч.

При этом, если учесть еще не устранённые уязвимости, то среднее время их жизни составит **135 дней**. Это говорит о том, что несмотря на наличие локальных вспышек и хайповых новостей, администраторам скорее свойственно просто установить продукт и забыть о нем.

Enterprise VS Open-Source

До построения следующих диаграмм, у нас была гипотеза: существует зависимость принадлежности продукта категории Enterprise или Open-Source и среднем временем жизни уязвимостей в нём. Одним из аргументов был тот факт, что в Enterprise-продуктах вендоры

тщательнее следят за безопасностью, уведомляют клиентов, и потому среднее время жизни уязвимости будет меньше, а в Open-Source такие процессы самотечны и, поэтому, время устранения больше. Помимо этого, такая тенденция уже наблюдалась для категории почтовых систем.



Сравнение среднего времени жизни в Enterprise и Open-Source продуктах

Однако как показала практика, если разбить продукты на эти две категории, то однозначно такой вывод сделать нельзя, и среднее время устранения все равно зависит от конкретного продукта и от конкретного вендора.

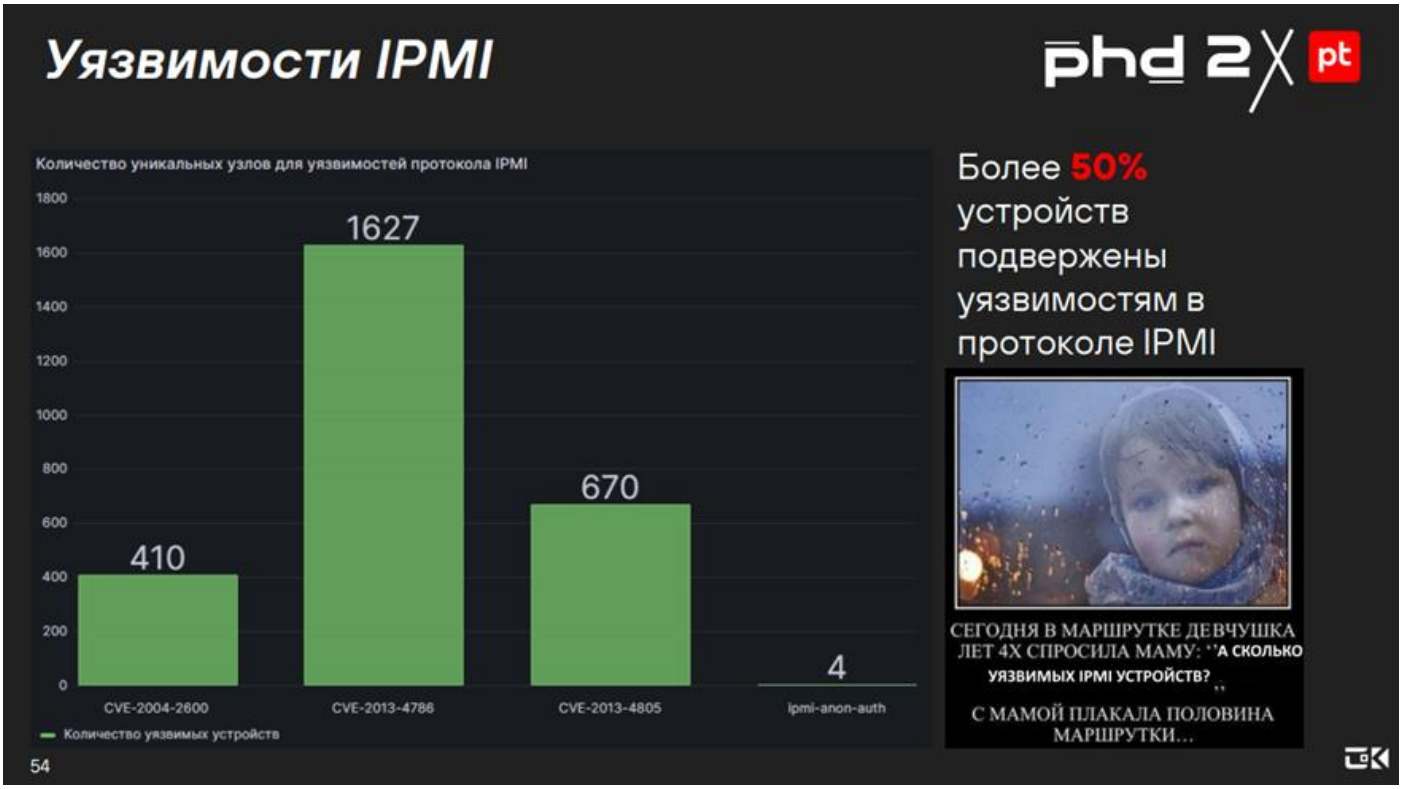
Back to the past: IPMI

В прошлом году мы выступали на PHD с докладом про уязвимости в различных сетевых устройствах: «Маленькие большие коробочки». Тут можно прочитать, а тут посмотреть.

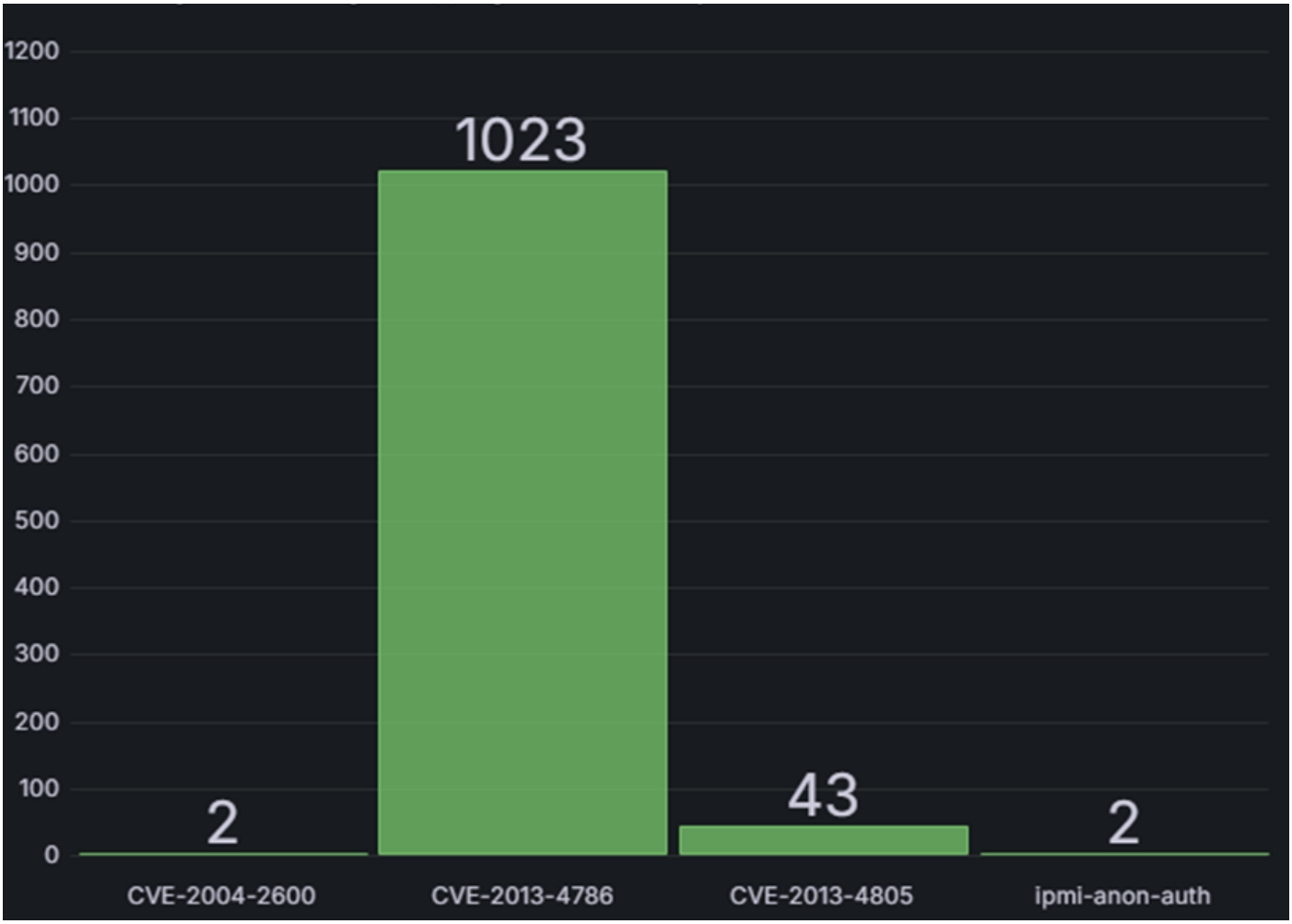
И, в частности, в этом докладе речь шла об уязвимостях протокола IPMI, который необходим для удаленного управления сервером. Во время того исследования выяснилось, что уязвимости, возраст которых составляет 15 и даже 20 лет весьма распространены.

Мы провели это исследование еще раз и, хорошая новость: мы побороли уязвимости 20-летней давности. Плохая: уязвимости 2013 года всё ещё на месте. Одна из них (CVE-2013-4785) позволяет, зная имя пользователя (а для таких устройств практически всегда существует пользователь admin), получить хэш пароля (а в протоколе IPMI используется MD5).

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337



Уязвимости в IPMI-устройствах, 2024 г.



Выводы

Анализ результатов подтверждает важность регулярного обновления ресурсов. Это может быть достигнуто путем централизованного реагирования и автоматизации обновлений, что особенно актуально для организаций с распределенной IT-инфраструктурой. Помимо этого, актуально совершенствование мониторинга уязвимостей с помощью механизмов автоматического выявления "забытых" инстансов.

Важность своевременного обновления подчеркивает и тот факт, что, несмотря на то, что крупные вендоры регулярно выпускают патчи, исправляющие новые уязвимости, общей тенденции быстрого обновления для их продуктов не наблюдается. При этом, несмотря на доступность кода, продукты категории Open-Source также не демонстрируют высокой скорости устранения уязвимостей.

Вышесказанное можно сформулировать в виде простых рекомендаций:

1. Знайте свой сетевой периметр.
2. Регулярно обновляйтесь.
3. Не выставляйте в Интернет то, чего там находиться не должно.

Приглашаем вас к нам в Telegram-канал, где мы публикуем информацию о новых уязвимостях с оценкой их распространённости в Интернете, а также делимся новостями с полей разработки СКИПА.

А если у вас есть мысли, наблюдения или опыт на тему “срока жизни” уязвимостей — делитесь в комментариях.