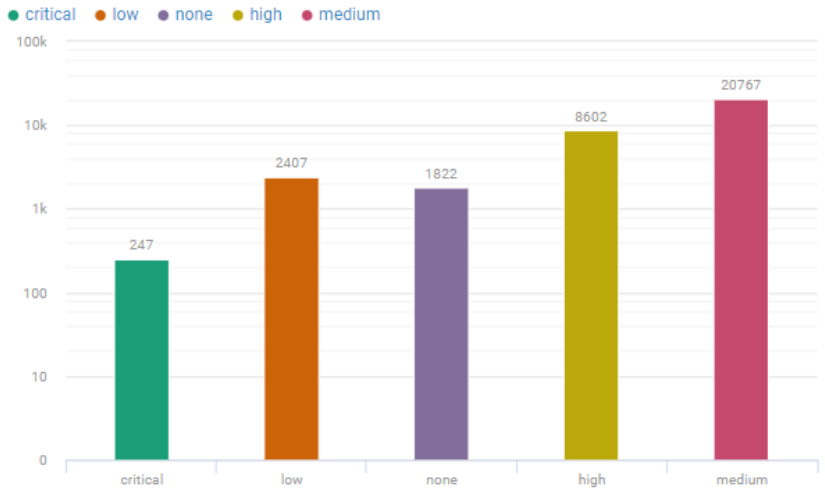
Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

1. Точечный отчёт по сканированию:

Уязвимости (по критичности)



Список уязвимостей

Уязвимость	Количество
aaa1 (192.168.0.248)	
Разглашение информации CVE-2017-3841 Cisco Cisco ACS	1 0 0
Межсайтовое выполнение сценариев CVE-2017-3838 Cisco Cisco ACS	1 0 0
Открытая переадресация CVE-2017-3840 Cisco Cisco ACS	1 0 0
Несанкционированный доступ на чтение CVE-2017-3839 Cisco Cisco ACS	1 0 0
aaa2 (192.168.0.247)	
Разглашение информации CVE-2017-3841 Cisco Cisco ACS	1 0 0
Межсайтовое выполнение сценариев CVE-2017-3838 Cisco Cisco ACS	1 0 0
Открытая переадресация CVE-2017-3840 Cisco Cisco ACS	1 0 0

aaa1 (192.168.0.248)

Разглашение информации CVE-2017-3841 Cisco Cisco ACS

Удаленно | Есть исправление | 1 | 0 | 0

Уязвимость в веб-интерфейсе системы контроля безопасного доступа Cisco Secure ACS позволяет неавторизованным злоумышленникам, действующим удаленно, получить доступ к конфиденциальной информации.

Дата публикации
15 февраля 2017, 03:00

Как исправить
Используйте рекомендации производителя:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-acs3

Ссылки
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-acs3

Статус	Уязвимость на активе	Обнаружена
Просрочено	aaa1 (192.168.0.248) Устранение: Плановое Cisco Cisco ACS 2.0.3.058	20 фев, 19:31

Межсайтовое выполнение сценариев CVE-2017-3838 Cisco Cisco ACS

Удаленно | Есть исправление | 1 | 0 | 0

Уязвимость в системе контроля безопасного доступа Cisco Secure ACS позволяет неавторизованным злоумышленникам, действующим удаленно, осуществить межсайтовое выполнение сценариев на основе объектной модели документа для пользователей, использующих веб-интерфейс уязвимой системы.

Дата публикации
15 февраля 2017, 03:00

Как исправить
Используйте рекомендации производителя:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-acs

Ссылки
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-acs

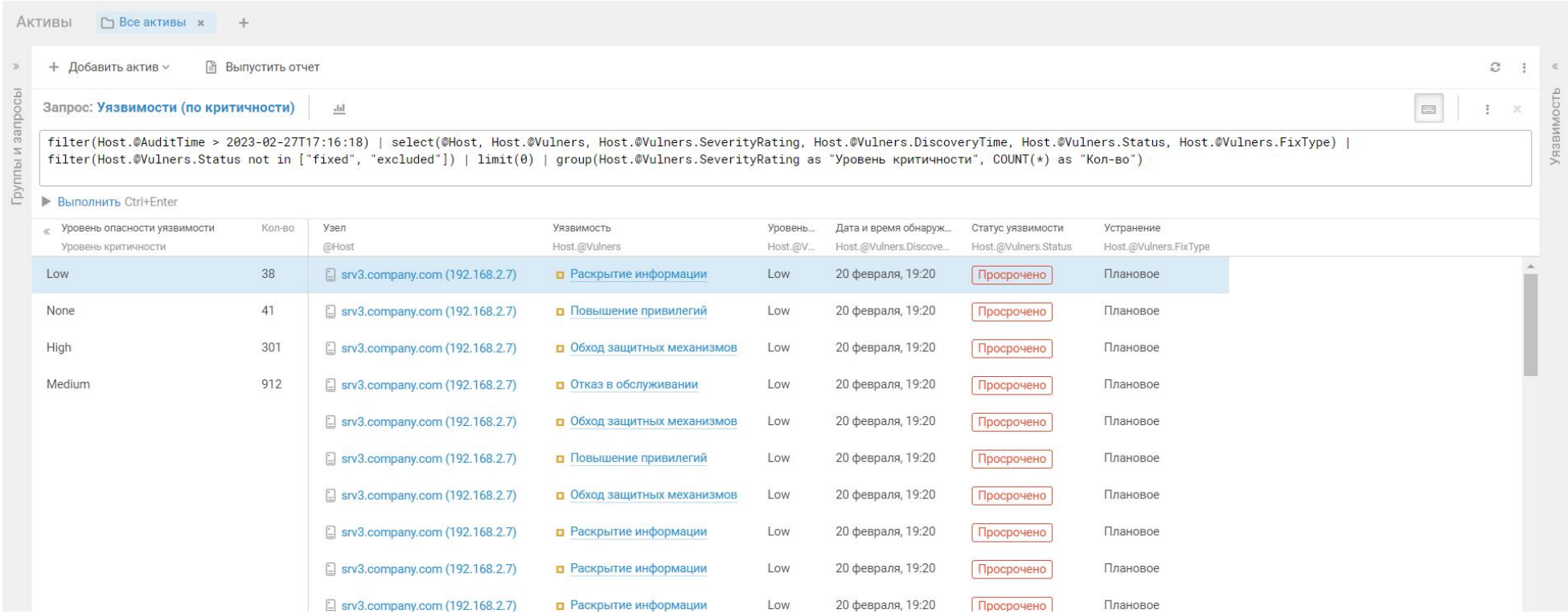
Виджет «Уязвимости (по критичности)»

Открываем вкладку «Активы» и нажимаем на иконку клавиатуры, чтобы перейти к текстовому редактированию запроса.

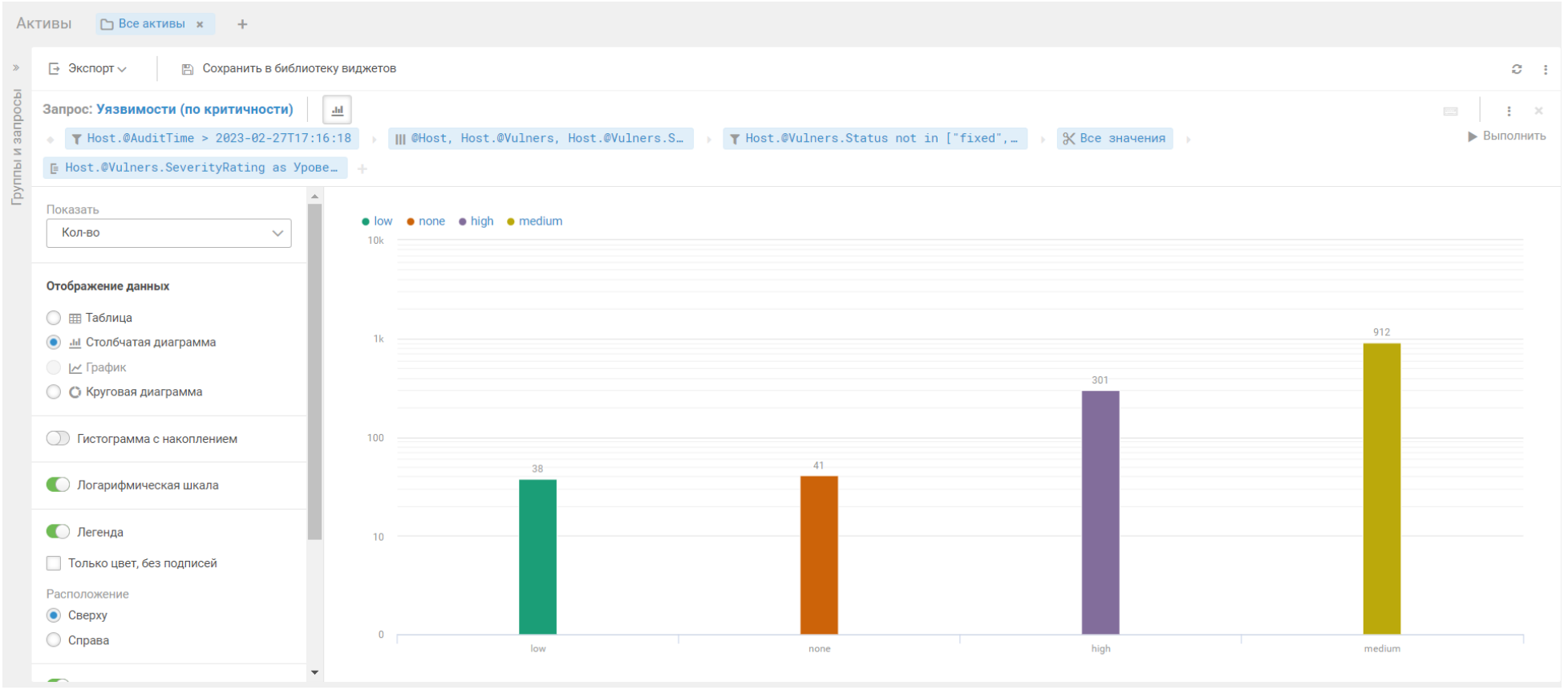
Вставляем и выполняем следующий запрос:

filter(Host.@AuditTime > 2023-02-27T17:16:18) | select(@Host, Host.@Vulners, Host.@Vulners.SeverityRating, Host.@Vulners.DiscoveryTime, Host.@Vulners.Status, Host.@Vulners.FixType) | filter(Host.@Vulners.Status not in ["fixed", "excluded"]) | limit(0) | group(Host.@Vulners.SeverityRating as "Уровень критичности", COUNT(*) as "Кол-во")

*Фильтр в начале запроса может задаваться параметрами Host.@AuditTime/Host.@PentestTime/Host.@UpdateTime в соответствии с целью выпуска отчёта



Переходим в режим создания виджета нажатием соответствующей иконки:



В разделе «Отображение данных» выбираем «Столбчатая диаграмма».

Включаем использование «Логарифмической шкалы» и «Подписи данных на диаграмме».

Сохраняем получившийся виджет в библиотеку виджетов нажатием соответствующей кнопки.

На вкладке «Система» -> «Отчёты» создаём новый отчёт без шаблона и добавляем виджет.

positive technologies

Виджет: «Список уязвимостей»

Добавляем стандартный виджет «Список уязвимостей».

В настройках виджета указываем:

На вкладке «Отображение»

1) «Данные для виджета» -> Отключить
2) «Группировка» -> Выбираем «По активу»
3) «Сортировка паспортов уязвимостей» -> Выбираем «Оценка по CVSS»
4) «Сортировка уязвимостей» -> Выбираем «Статус уязвимости»

На вкладке «Источник»

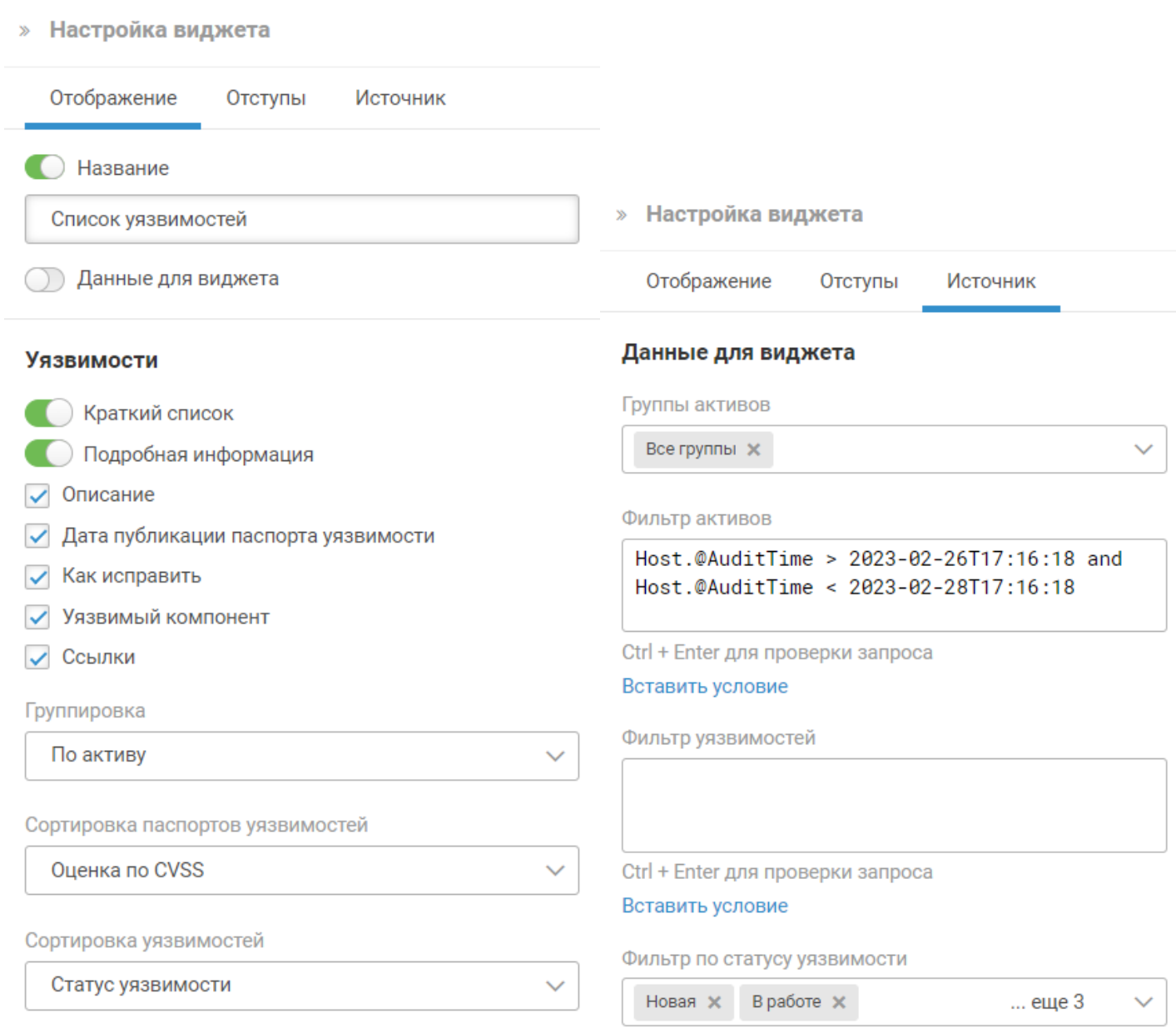
1) «Группы активов» -> Указываем группу активов, по которой запускалась задача сканирования, или выбираем «Все активы»
2) «Фильтр активов» -> Указываем фильтр по активам:

время аудита актива	Host.@AuditTime > 2023-02-26T17:16:18 and Host.@AuditTime < 2023-02-28T17:16:18
время пентеста актива	Host.@PentestTime > now() - 1d
время обновления актива: пентест/аудит/из событий	Host.@UpdateTime > 2023-02-27T17:16:18
IP-адрес/Вхождение в подсеть	Host.IpAddress in 192.168.2.0/24 or Host.IpAddress = 192.168.2.12
FDQN	Host.Fqdn like '%.company.com' or Host.Fqdn = 'fw10.company.com'

3) «Фильтр уязвимостей» -> Указываем фильтр по времени действий, направленных на работу с уязвимостями:

время обнаружения уязвимостей	Host.@Vulners.DiscoveryTime > 2023-02-26T11:16:18
время обновления уязвимостей/их статуса	Host.@Vulners.StatusUpdateTime > 2023-02-26T11:16:18
время устранения уязвимостей	Host.@Vulners.LastFixTime > now() - 30d

4) «Фильтр по статусу уязвимости» -> Выбираем все статусы, кроме «Устранена» и «Исключена»


» Настройка виджета
Отображение
Отступы
Источник
Название
Список уязвимостей
Данные для виджета
Уязвимости
Краткий список
Подробная информация
Описание
Дата публикации паспорта уязвимости
Как исправить
Уязвимый компонент
Ссылки
Группировка
По активу
Сортировка паспортов уязвимостей
Оценка по CVSS
Сортировка уязвимостей
Статус уязвимости
» Настройка виджета
Отображение
Отступы
Источник
Данные для виджета
Группы активов
Все группы
Фильтр активов
Host.@AuditTime > 2023-02-26T17:16:18 and
Host.@AuditTime < 2023-02-28T17:16:18
Ctrl + Enter для проверки запроса
Вставить условие
Фильтр уязвимостей
Ctrl + Enter для проверки запроса
Вставить условие
Фильтр по статусу уязвимости
Новая
В работе
... еще 3

2. Дифференциальный отчёт

Динамика уязвимостей (по критичности)

Severity	23 февраля, 21:55	24 февраля, 21:55	25 февраля, 21:55	26 февраля, 21:55	27 февраля, 21:55	28 февраля, 21:55
critical	678	678	678	678	678	678
high	14943	14943	14943	14947	14947	14947
none	2372	2372	2372	2372	2372	2372
medium	35158	35158	35158	35181	35181	35181
low	5425	5425	5425	5425	5425	5425

Всего: 5

Общая статистика по узлам

@Host	Устранённые уязвимости	Новые уязвимости	Сохранившиеся без изменений	Сохранившиеся с изменениями
switch3.company.com (192.168.0.233)	*null*	*null*	*null*	12
switch2.company.com (192.168.0.211)	*null*	*null*	12	*null*
srv9.company.com (192.168.0.14)	*null*	13	1140	13
srv7.company.com (192.168.2.12)	44	22	1144	26
srv6.company.com (192.168.0.11)	3	15	1014	76
srv4.company.com (192.168.1.9)	4	*null*	*null*	*null*
srv3.company.com (192.168.2.7)	4	21	1189	70
srv2.company.com (192.168.0.6)	*null*	*null*	106	*null*
srv13.company.com (192.168.2.8)	2	14	3413	63
srv12.company.com (192.168.0.17)	*null*	12	6009	12
srv11.company.com (192.168.2.16)	*null*	26	792	26

Устранённые уязвимости (за 7 дней)

Уязвимость	Количество		
srv10.company.com (192.168.2.15)			
Microsoft Microsoft .NET Framework			
Удаленное выполнение кода CVE-2022-26929	0	2	0
srv13.company.com (192.168.2.8)			
Microsoft Microsoft .NET Framework			
Удаленное выполнение кода CVE-2022-26929	0	2	0
srv3.company.com (192.168.2.7)			
Microsoft Microsoft .NET Framework			
Удаленное выполнение кода CVE-2022-26929	0	4	0
srv7.company.com (192.168.2.12)			
Debian Project Debian			
CVE-2019-10207 CVE-2019-10207	0	1	0
CVE-2019-0155	0	1	0
CVE-2019-0154 CVE-2019-0154	0	1	0
Раскрытие информации CVE-2019-11135	0	1	0
Отказ в обслуживании CVE-2018-12207	0	1	0
CVE-2019-14821 CVE-2019-14821	0	1	0
CVE-2019-14835 CVE-2019-14835	0	1	0
CVE-2019-15902 CVE-2019-15902	0	1	0
CVE-2019-15117 CVE-2019-15117	0	1	0
CVE-2019-15118 CVE-2019-15118	0	1	0
Разглашение информации CVE-2019-1125	0	1	0
CVE-2019-14283 CVE-2019-14283	0	1	0

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

srv10.company.com (192.168.2.15)

Microsoft Microsoft .NET Framework

Удаленное выполнение кода CVE-2022-26929 Microsoft Microsoft .NET Framework

Есть исправление | 0 | 2 | 0

Уязвимость в .NET Framework позволяет злоумышленникам, действующим удаленно, выполнить произвольный код и оказать воздействие на систему.

Дата публикации
13 сентября 2022, 03:00

Как исправить
Используйте рекомендации производителя:
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26929

Статус	Уязвимость на активе	Обнаружена
Устранена	srv10.company.com (192.168.2.15) (Исправлено ложное срабатывание) Устранение: Нет политики C:\Windows\Microsoft.net\Framework\V3.5\ Microsoft Microsoft .NET Framework 3.5	20 фев, 19:20
	srv10.company.com (192.168.2.15) (Исправлено ложное срабатывание) Устранение: Нет политики C:\Windows\Microsoft.net\Framework64\V3.5\ Microsoft Microsoft .NET Framework 3.5	20 фев, 19:20

Новые уязвимости (за 7 дней)

Уязвимость	Количество		
srv11.company.com (192.168.2.16)			
Debian Project curl			
Уязвимость CVE-2023-23916 CVE-2023-23916	1	0	0
Debian Project git			
Уязвимость CVE-2023-23946 CVE-2023-23946	1	0	0
Уязвимость CVE-2023-22490 CVE-2023-22490	1	0	0
Debian Project git-man			
Уязвимость CVE-2023-23946 CVE-2023-23946	1	0	0
Уязвимость CVE-2023-22490 CVE-2023-22490	1	0	0
Debian Project libcurl3-gnutls			
Уязвимость CVE-2023-23916 CVE-2023-23916	1	0	0
Debian Project syslog-ng-core			
Уязвимость CVE-2022-38725 CVE-2022-38725	1	0	0
Debian Project syslog-ng-mod-sql			
Уязвимость CVE-2022-38725 CVE-2022-38725	1	0	0
srv7.company.com (192.168.2.12)			
Debian Project curl			
Уязвимость CVE-2023-23916 CVE-2023-23916	1	0	0
Debian Project libcurl3-gnutls			
Уязвимость CVE-2023-23916 CVE-2023-23916	1	0	0

Debian Project git

Уязвимость CVE-2023-23946 CVE-2023-23946 Debian Project git

Удаленно | Есть исправление | 1 | 0 | 0

Уязвимость в git-scm git

Дата публикации
14 февраля, 03:00

Как исправить
Проблема может быть решена обновлением операционной системы до следующих версий пакетов в зависимости от архитектуры:
Debian GNU/Linux 10:
noarch:
git - 1:2.20.1-2+deb10u8
git-all - 1:2.20.1-2+deb10u8
git-cvs - 1:2.20.1-2+deb10u8
git-daemon-run - 1:2.20.1-2+deb10u8
git-daemon-sysvinit - 1:2.20.1-2+deb10u8
git-doc - 1:2.20.1-2+deb10u8...
Развернуть

Ссылки
https://github.com/git/git/commit/c867e4fa180bec4750e9b54eb10f459030dbebfd
https://github.com/git/git/security/advisories/GHSA-r87m-v37r-cwfh

Статус	Уязвимость на активе	Обнаружена
Новая	srv11.company.com (192.168.2.16) Устранение: Нет политики Debian Project git 1:2.1.4-2.1+deb8u2	1 мар, 11:18

Сохранившиеся без изменений (за 7 дней)

Уязвимость	Количество		
srv10.company.com (192.168.2.15)			
Igor Pavlov 7-Zip			
Выполнение произвольного кода CVE-2018-10115	1	0	0
Microsoft Microsoft .NET Framework			
Удаленное выполнение кода CVE-2022-41089	2	0	0
Отказ в обслуживании CVE-2022-30130	2	0	0
Отказ в обслуживании CVE-2022-26832	2	0	0
Отказ в обслуживании CVE-2022-21911	2	0	0
Раскрытие информации CVE-2020-16937	2	0	0
Повышение привилегий CVE-2020-1476	2	0	0
Удаленное выполнение кода CVE-2020-1046	2	0	0
Удаленное выполнение кода CVE-2020-1147	2	0	0
Отказ в обслуживании CVE-2020-1108	2	0	0
Удаленное выполнение кода CVE-2020-0646	2	0	0
Удаленное выполнение кода CVE-2020-0605	2	0	0
Удаленное выполнение кода CVE-2020-0606	2	0	0
Повышение привилегий CVE-2019-1142	2	0	0
Удаленное выполнение кода CVE-2019-1113	2	0	0

Здесь показаны первые 15 уязвимостей. В отчет войдет таблица целиком (8362 строки).

srv10.company.com (192.168.2.15)

Igor Pavlov 7-Zip

Выполнение произвольного кода CVE-2018-10115 Igor Pavlov 7-Zip

Есть исправление | 1 | 0 | 0

Использование неинициализированной памяти в 7-Zip, связанное с некорректной логикой инициализации объектов декодера RAR, позволяет злоумышленникам, действующим удаленно, вызвать отказ в обслуживании (ошибку сегментации) или выполнить произвольный код с помощью специально сформированного RAR-архива.

Дата публикации
2 мая 2018, 03:00

Как исправить
Для устранения уязвимости необходимо установить последнюю версию продукта, соответствующую используемой платформе. Необходимую информацию можно получить по адресу:
http://www.7-zip.org/

Статус	Уязвимость на активе	Обнаружена
Новая	srv10.company.com (192.168.2.15) Устранение: Нет политики C:\Program files\7-zip\ Igor Pavlov 7-Zip 18.01	20 фев, 19:20

Сохранившиеся с изменениями (за 7 дней)

Уязвимость	Количество		
srv11.company.com (192.168.2.16)			
Debian Project curl			
Уязвимость CVE-2023-23916 CVE-2023-23916	1	0	0
Debian Project git			
Уязвимость CVE-2023-23946 CVE-2023-23946	1	0	0
Уязвимость CVE-2023-22490 CVE-2023-22490	1	0	0
Debian Project git-man			
Уязвимость CVE-2023-23946 CVE-2023-23946	1	0	0
Уязвимость CVE-2023-22490 CVE-2023-22490	1	0	0
Debian Project libcurl3-gnutls			
Уязвимость CVE-2023-23916 CVE-2023-23916	1	0	0
Debian Project libgnutls30			
Уязвимость CVE-2023-0361 CVE-2023-0361	1	0	0
Debian Project syslog-ng-core			
Уязвимость CVE-2022-38725 CVE-2022-38725	1	0	0
Debian Project syslog-ng-mod-sql			
Уязвимость CVE-2022-38725 CVE-2022-38725	1	0	0
srv7.company.com (192.168.2.12)			
Debian Project curl			
Уязвимость CVE-2023-23916 CVE-2023-23916	1	0	0
Debian Project libcurl3-gnutls			
Уязвимость CVE-2023-23916 CVE-2023-23916	1	0	0

Debian Project syslog-ng-core

Уязвимость CVE-2022-38725 CVE-2022-38725 Debian Project syslog-ng-core

Удаленно | Есть исправление | 1 | 0 | 0

Уязвимость в oneidentity syslog-ng, oneidentity syslog-ng store box

Дата публикации
23 января, 03:00

Как исправить
Проблема может быть решена обновлением операционной системы до следующих версий пакетов в зависимости от архитектуры:
Debian GNU/Linux 10:
noarch:
syslog-ng - 3.19.1-5+deb10u1
syslog-ng-core - 3.19.1-5+deb10u1
syslog-ng-dbg - 3.19.1-5+deb10u1
syslog-ng-dev - 3.19.1-5+deb10u1
syslog-ng-mod-add-contextual-data - 3.19.1-5+deb10u1
syslog-ng-mod-amqp - 3.19.1-5+deb10u1...
Развернуть

Ссылки
https://github.com/syslog-ng/syslog-ng/security/advisories/GHSA-7932-4fc6-pvmc
https://lists.balabit.hu/pipermail/syslog-ng/
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/J3TZ7
https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/QU36I

Статус	Уязвимость на активе	Обнаружена
Новая	srv11.company.com (192.168.2.16)	7 мар, 09:59
	Устранение: Нет политики	
	Debian Project syslog-ng-core 3.5.6-2+b1	

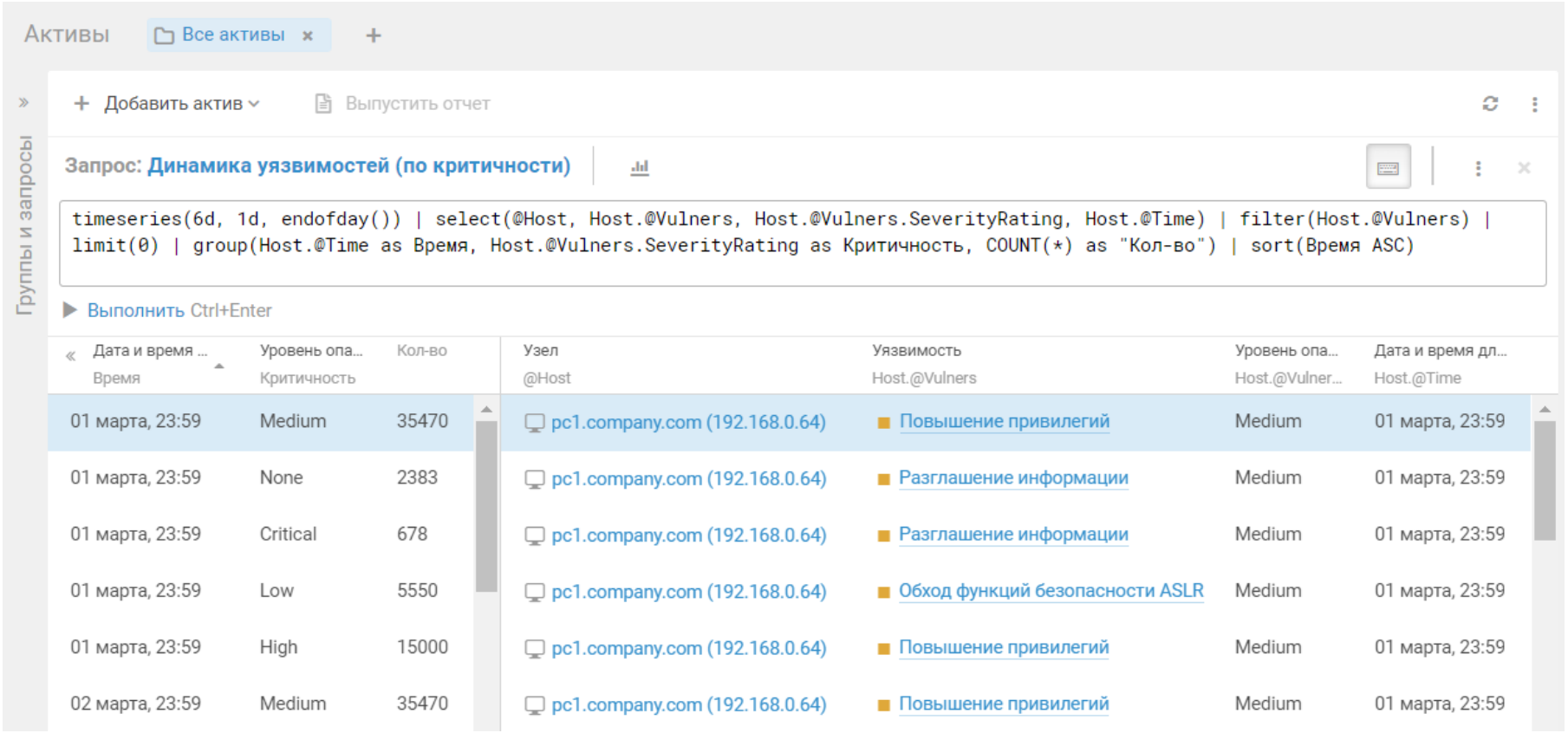
Виджет: «Динамика уязвимостей (по критичности)»

Переходим на вкладку «Активы» и нажимаем на иконку клавиатуры, чтобы перейти к текстовому редактированию запроса.

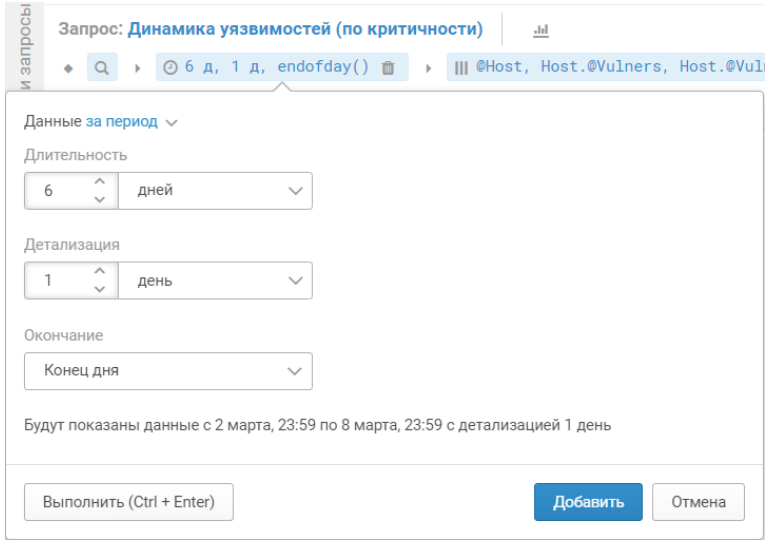
Вставляем и выполняем следующий запрос:

timeseries(6d, 1d, endofday()) | select(@Host, Host.@Vulners, Host.@Vulners.SeverityRating, Host.@Time) | filter(Host.@Vulners) | limit(0) | group(Host.@Time as Время, Host.@Vulners.SeverityRating as Критичность, COUNT(*) as "Кол-во") | sort(Время ASC)

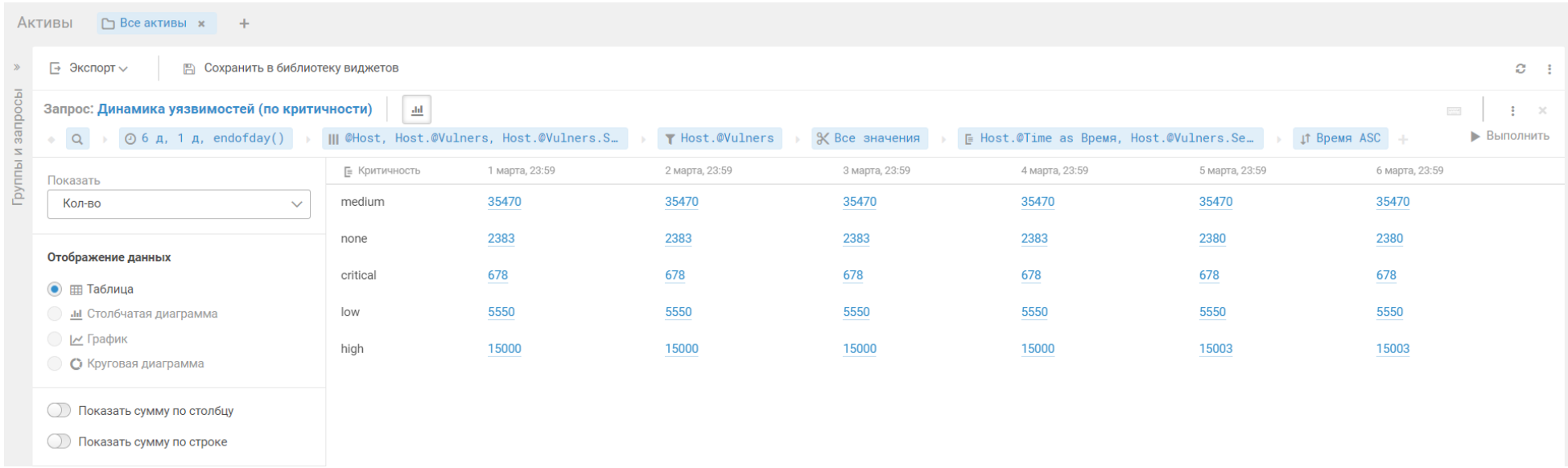
*Временную функцию timeseries можно настраивать в соответствии с периодом, за который хотим получить дифференциальный отчёт



Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями



Переходим в режим создания виджета нажатием соответствующей иконки:



positive technologies

Сохраняем получившийся виджет в библиотеку виджетов нажатием соответствующей кнопки.

На вкладке «Система» -> «Отчёты» создаём новый отчёт без шаблона и добавляем виджет.

Виджет: «Общая статистика по узлам»

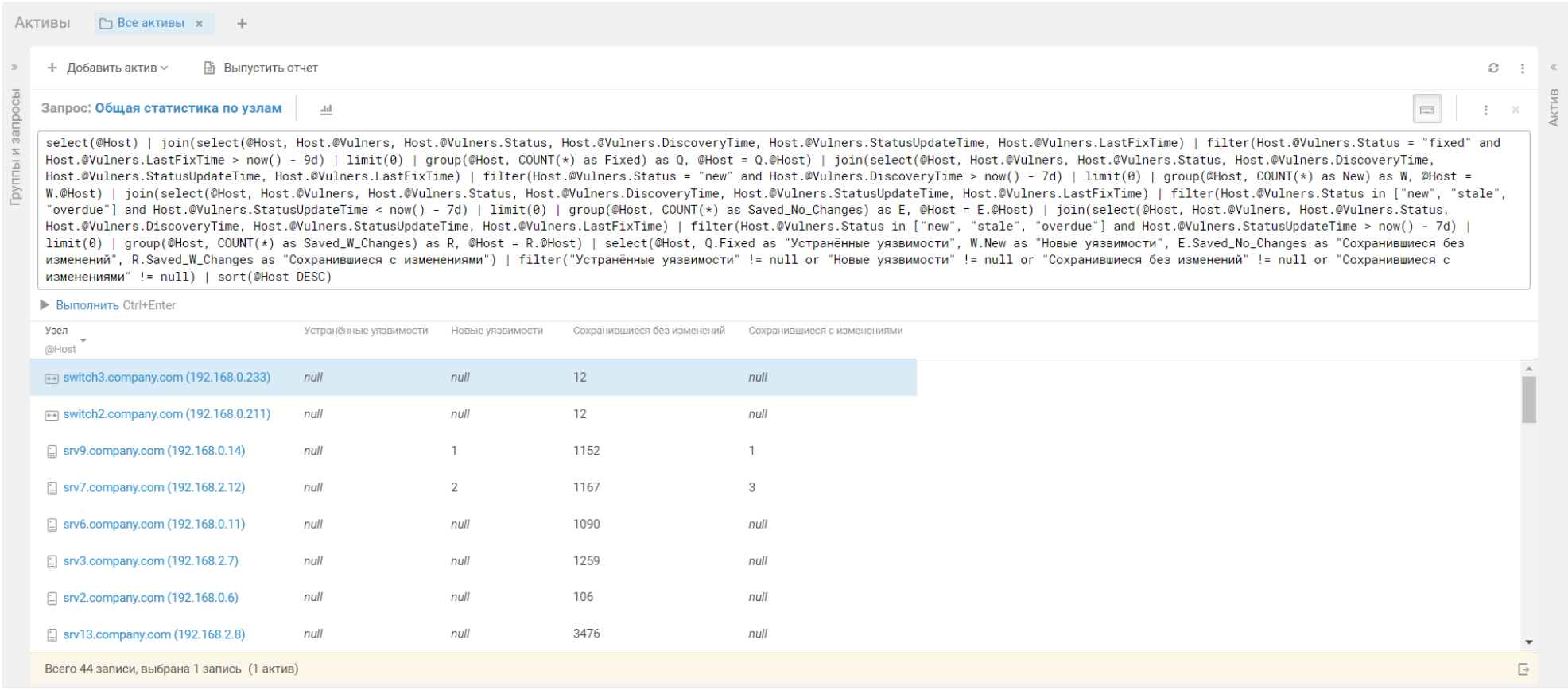
Переходим на вкладку «Активы» и нажимаем на иконку клавиатуры, чтобы перейти к текстовому редактированию запроса.

Вставляем и выполняем следующий запрос:

```
select(@Host) | join(select(@Host, Host.@Vulners, Host.@Vulners.Status, Host.@Vulners.DiscoveryTime, Host.@Vulners.StatusUpdateTime, Host.@Vulners.LastFixTime) | filter(Host.@Vulners.Status = "fixed" and Host.@Vulners.LastFixTime > now() - 7d) | limit(0) | group(@Host, COUNT(*) as Fixed) as Q, @Host = Q.@Host) | join(select(@Host, Host.@Vulners, Host.@Vulners.Status, Host.@Vulners.DiscoveryTime, Host.@Vulners.StatusUpdateTime, Host.@Vulners.LastFixTime) | filter(Host.@Vulners.Status = "new" and Host.@Vulners.DiscoveryTime > now() - 7d) | limit(0) | group(@Host, COUNT(*) as New) as W, @Host = W.@Host) | join(select(@Host, Host.@Vulners, Host.@Vulners.Status, Host.@Vulners.DiscoveryTime, Host.@Vulners.StatusUpdateTime, Host.@Vulners.LastFixTime) | filter(Host.@Vulners.Status in ["new", "stale", "overdue"] and Host.@Vulners.StatusUpdateTime < now() - 7d) | limit(0) | group(@Host, COUNT(*) as Saved_No_Changes) as E, @Host = E.@Host) | join(select(@Host, Host.@Vulners, Host.@Vulners.Status, Host.@Vulners.DiscoveryTime, Host.@Vulners.StatusUpdateTime, Host.@Vulners.LastFixTime) | filter(Host.@Vulners.Status in ["new", "stale", "overdue"] and Host.@Vulners.StatusUpdateTime > now() - 7d) | limit(0) | group(@Host, COUNT(*) as Saved_W_Changes) as R, @Host = R.@Host) | select(@Host, Q.Fixed as "Устранённые уязвимости", W.New as "Новые уязвимости", E.Saved_No_Changes as "Сохранившиеся без изменений", R.Saved_W_Changes as "Сохранившиеся с изменениями") | filter("Устранённые уязвимости" != null or "Новые уязвимости" != null or "Сохранившиеся без изменений" != null or "Сохранившиеся с изменениями" != null) | sort(@Host DESC)
```

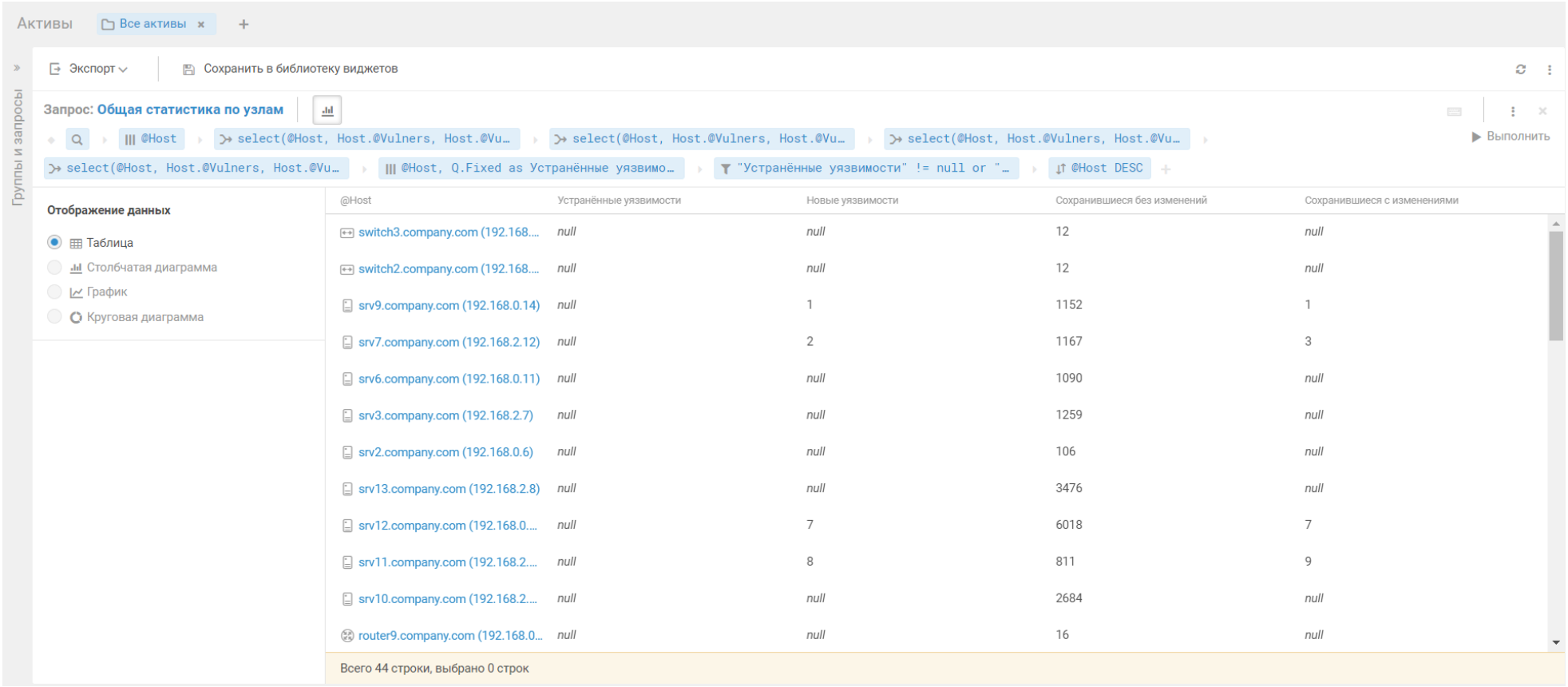
*В данном примере приведён запрос сбора статистики по уязвимостям за последние 7 дней. При необходимости пользователь может изменить значение «now() - 7d» на своё.

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями



positive technologies

Переходим в режим создания виджета нажатием соответствующей иконки:



Сохраняем получившийся виджет в библиотеку виджетов нажатием соответствующей кнопки.

На вкладке «Система» -> «Отчёты» выбираем созданный ранее отчёт и добавляем в него виджет.

Виджет: «Устранённые уязвимости (за 7 дней)»

Добавляем стандартный виджет «Список уязвимостей».

В настройках виджета указываем:

На вкладке «Отображение»

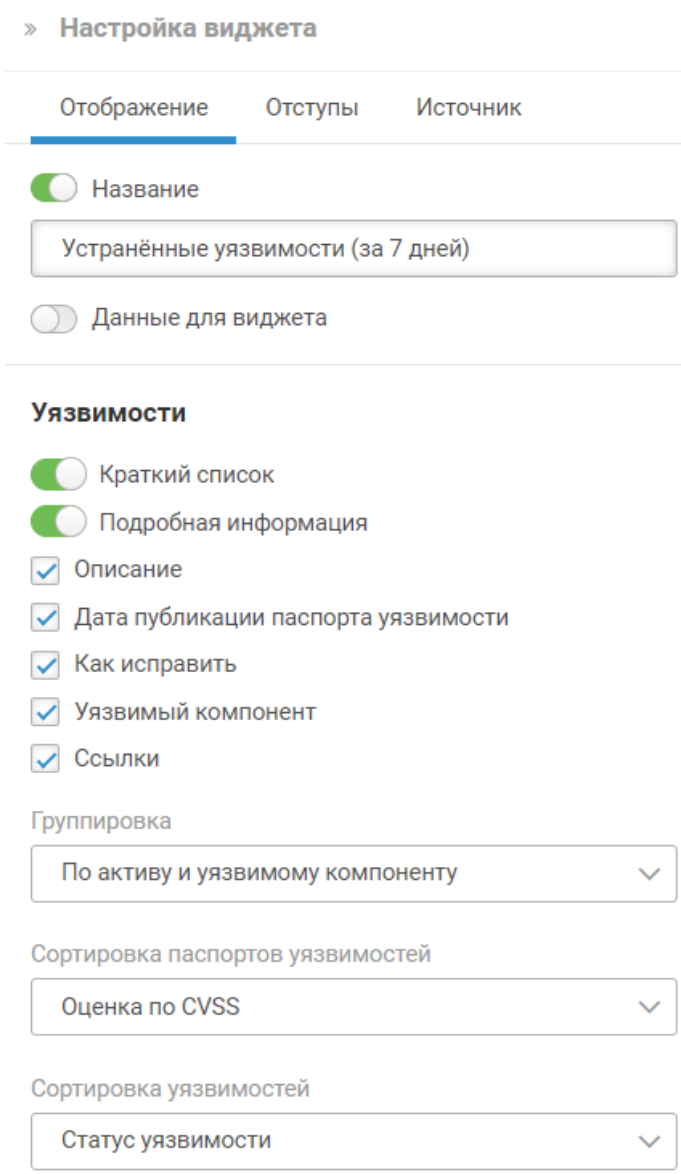
1) «Данные для виджета» -> Отключить
2) «Группировка» -> Выбираем «По активу и уязвимому компоненту»
3) «Сортировка паспортов уязвимостей» -> Выбираем «Оценка по CVSS»
4) «Сортировка уязвимостей» -> Выбираем «Статус уязвимости»

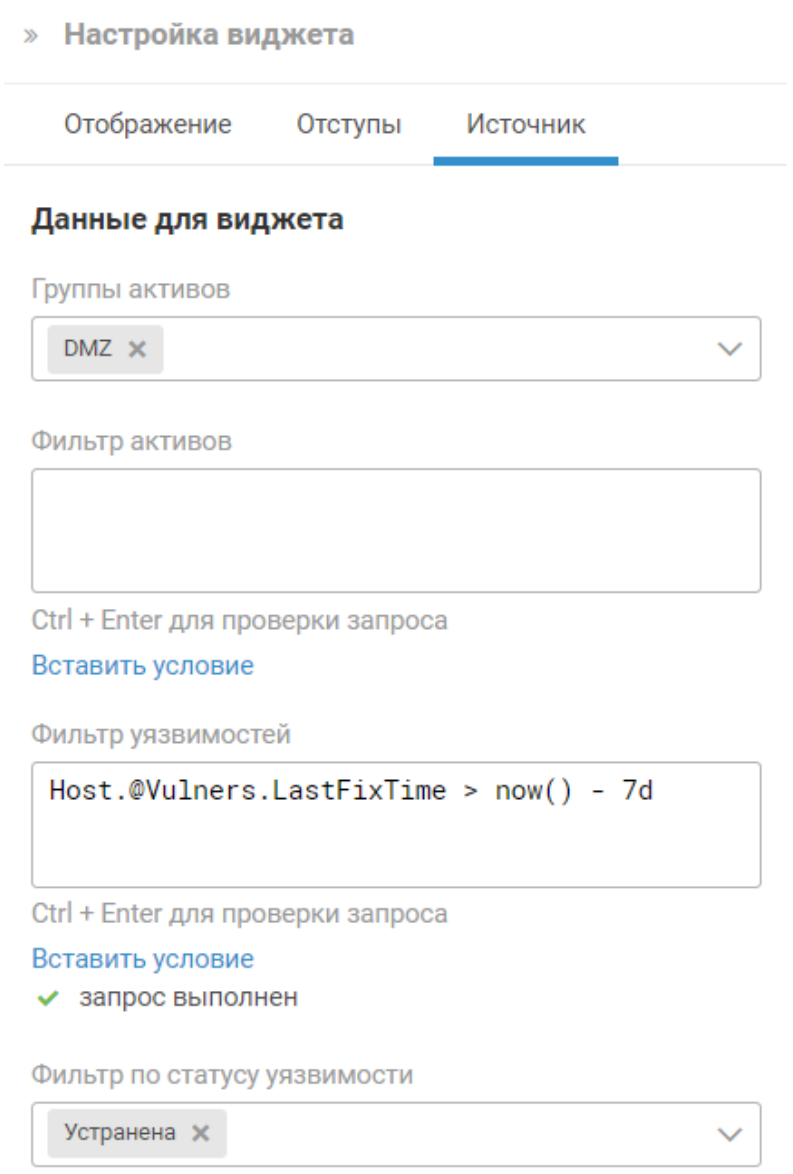
На вкладке «Источник»

1) «Группы активов» -> Указываем группу активов, по которой хотим выпустить дифференциальный отчёт, или выбираем «Все активы»
2) «Фильтр уязвимостей» -> Указываем фильтр, чтобы оставить уязвимости, которые были устранены за последние 7 дней:

```
Host.@Vulners.LastFixTime > now() - 7d
```

3) «Фильтр по статусу уязвимости» -> Выбираем только статус «Устранена»


» Настройка виджета
Отображение
Отступы
Источник
Название
Устранённые уязвимости (за 7 дней)
Данные для виджета
Уязвимости
Краткий список
Подробная информация
Описание
Дата публикации паспорта уязвимости
Как исправить
Уязвимый компонент
Ссылки
Группировка
По активу и уязвимому компоненту
Сортировка паспортов уязвимостей
Оценка по CVSS
Сортировка уязвимостей
Статус уязвимости


» Настройка виджета
Отображение
Отступы
Источник
Данные для виджета
Группы активов
DMZ
Фильтр активов
Ctrl + Enter для проверки запроса
Вставить условие
Фильтр уязвимостей
Host.@Vulners.LastFixTime > now() - 7d
Ctrl + Enter для проверки запроса
Вставить условие
запрос выполнен
Фильтр по статусу уязвимости
Устранена

Виджет: «Новые уязвимости (за 7 дней)»

Добавляем стандартный виджет «Список уязвимостей».

В настройках виджета указываем:

На вкладке «Отображение»

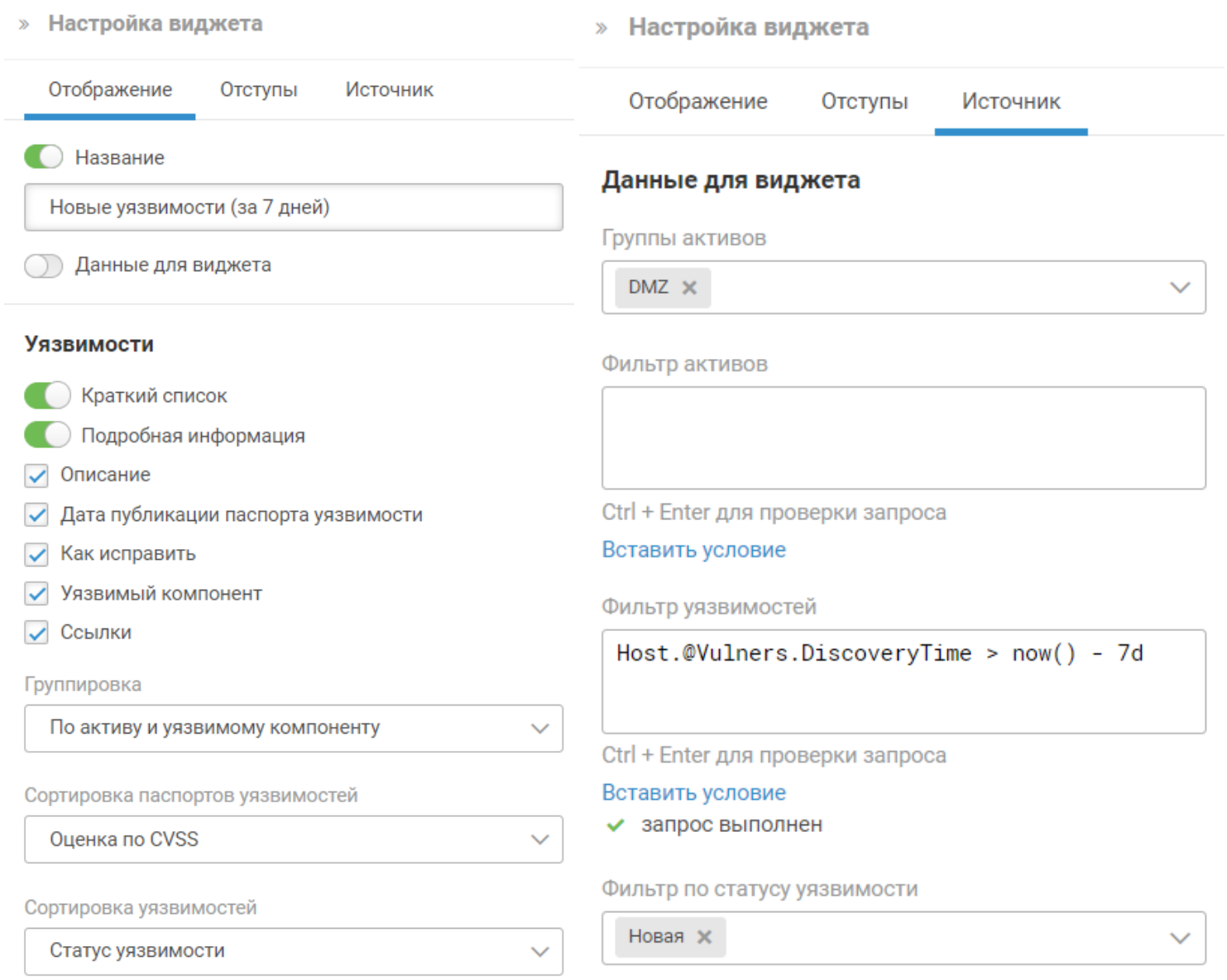
1) «Данные для виджета» -> Отключить
2) «Группировка» -> Выбираем «По активу и уязвимому компоненту»
3) «Сортировка паспортов уязвимостей» -> Выбираем «Оценка по CVSS»
4) «Сортировка уязвимостей» -> Выбираем «Статус уязвимости»

На вкладке «Источник»

1) «Группы активов» -> Указываем группу активов, по которой хотим выпустить дифференциальный отчёт, или выбираем «Все активы»
2) «Фильтр уязвимостей» -> Указываем фильтр, чтобы оставить уязвимости, которые были обнаружены за последние 7 дней:

```
Host.@Vulners.DiscoveryTime > now() - 7d
```

3) «Фильтр по статусу уязвимости» -> Выбираем только статус «Новая»


» Настройка виджета
Отображение
Отступы
Источник
Название
Новые уязвимости (за 7 дней)
Данные для виджета
Уязвимости
Краткий список
Подробная информация
Описание
Дата публикации паспорта уязвимости
Как исправить
Уязвимый компонент
Ссылки
Группировка
По активу и уязвимому компоненту
Сортировка паспортов уязвимостей
Оценка по CVSS
Сортировка уязвимостей
Статус уязвимости
» Настройка виджета
Отображение
Отступы
Источник
Данные для виджета
Группы активов
DMZ
Фильтр активов
Ctrl + Enter для проверки запроса
Вставить условие
Фильтр уязвимостей
Host.@Vulners.DiscoveryTime > now() - 7d
Ctrl + Enter для проверки запроса
Вставить условие
запрос выполнен
Фильтр по статусу уязвимости
Новая

Виджет: «Сохранившиеся без изменений (за 7 дней)»

Добавляем стандартный виджет «Список уязвимостей».

В настройках виджета указываем:

На вкладке «Отображение»

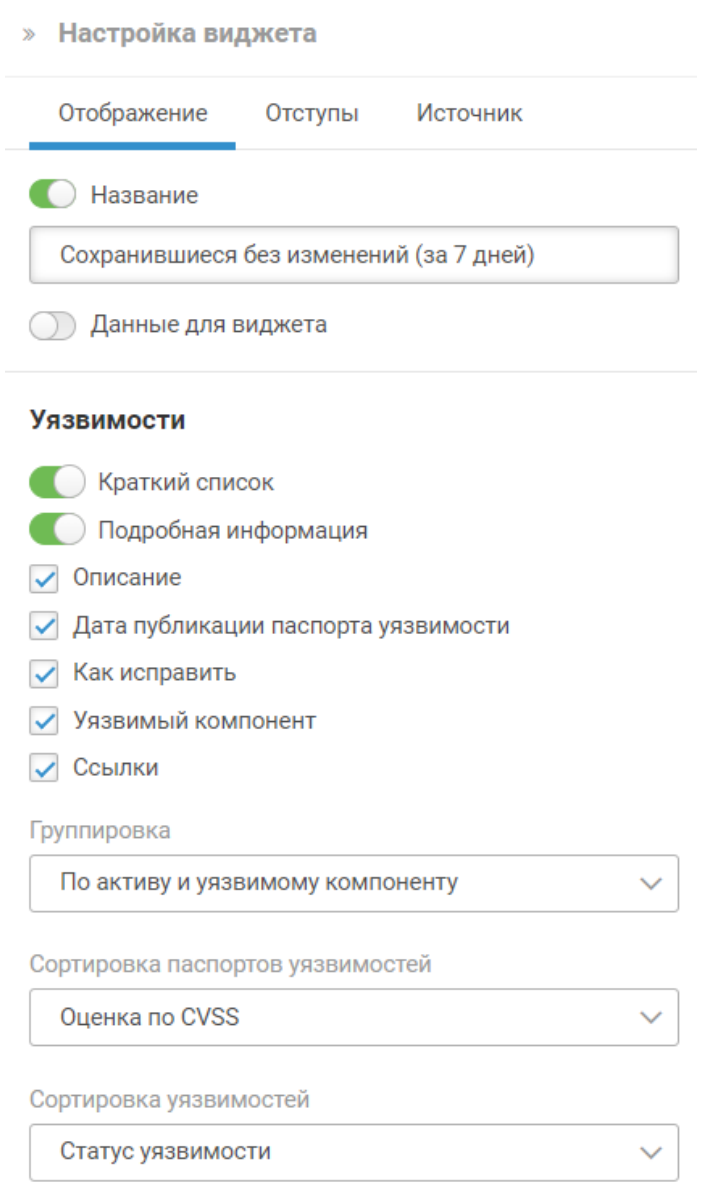
1) «Данные для виджета» -> Отключить
2) «Группировка» -> Выбираем «По активу и уязвимому компоненту»
3) «Сортировка паспортов уязвимостей» -> Выбираем «Оценка по CVSS»
4) «Сортировка уязвимостей» -> Выбираем «Статус уязвимости»

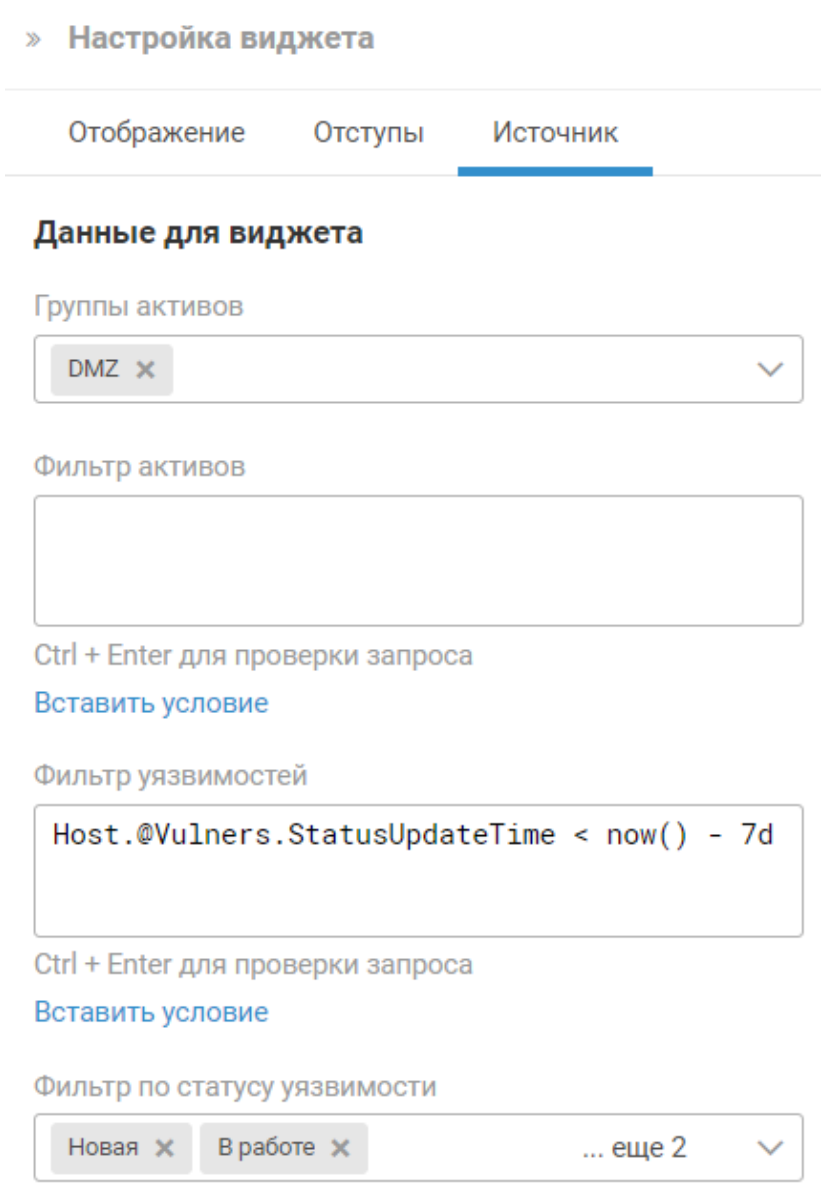
На вкладке «Источник»

1) «Группы активов» -> Указываем группу активов, по которой хотим выпустить дифференциальный отчёт, или выбираем «Все активы»
2) «Фильтр уязвимостей» -> Указываем фильтр, чтобы оставить уязвимости, статус которых не обновлялся за последние 7 дней:

```
Host.@Vulners.StatusUpdateTime < now() - 7d
```

3) «Фильтр по статусу уязвимости» -> Выбираем все статусы, кроме «Исправляется», «Исключена», «Устранена»


» Настройка виджета
Отображение
Отступы
Источник
Название
Сохранившиеся без изменений (за 7 дней)
Данные для виджета
Уязвимости
Краткий список
Подробная информация
Описание
Дата публикации паспорта уязвимости
Как исправить
Уязвимый компонент
Ссылки
Группировка
По активу и уязвимому компоненту
Сортировка паспортов уязвимостей
Оценка по CVSS
Сортировка уязвимостей
Статус уязвимости


» Настройка виджета
Отображение
Отступы
Источник
Данные для виджета
Группы активов
DMZ
Фильтр активов
Ctrl + Enter для проверки запроса
Вставить условие
Фильтр уязвимостей
Host.@Vulners.StatusUpdateTime < now() - 7d
Ctrl + Enter для проверки запроса
Вставить условие
Фильтр по статусу уязвимости
Новая
В работе
... еще 2

Виджет: «Сохранившиеся с изменениями (за 7 дней)»

Добавляем стандартный виджет «Список уязвимостей».

В настройках виджета указываем:

На вкладке «Отображение»

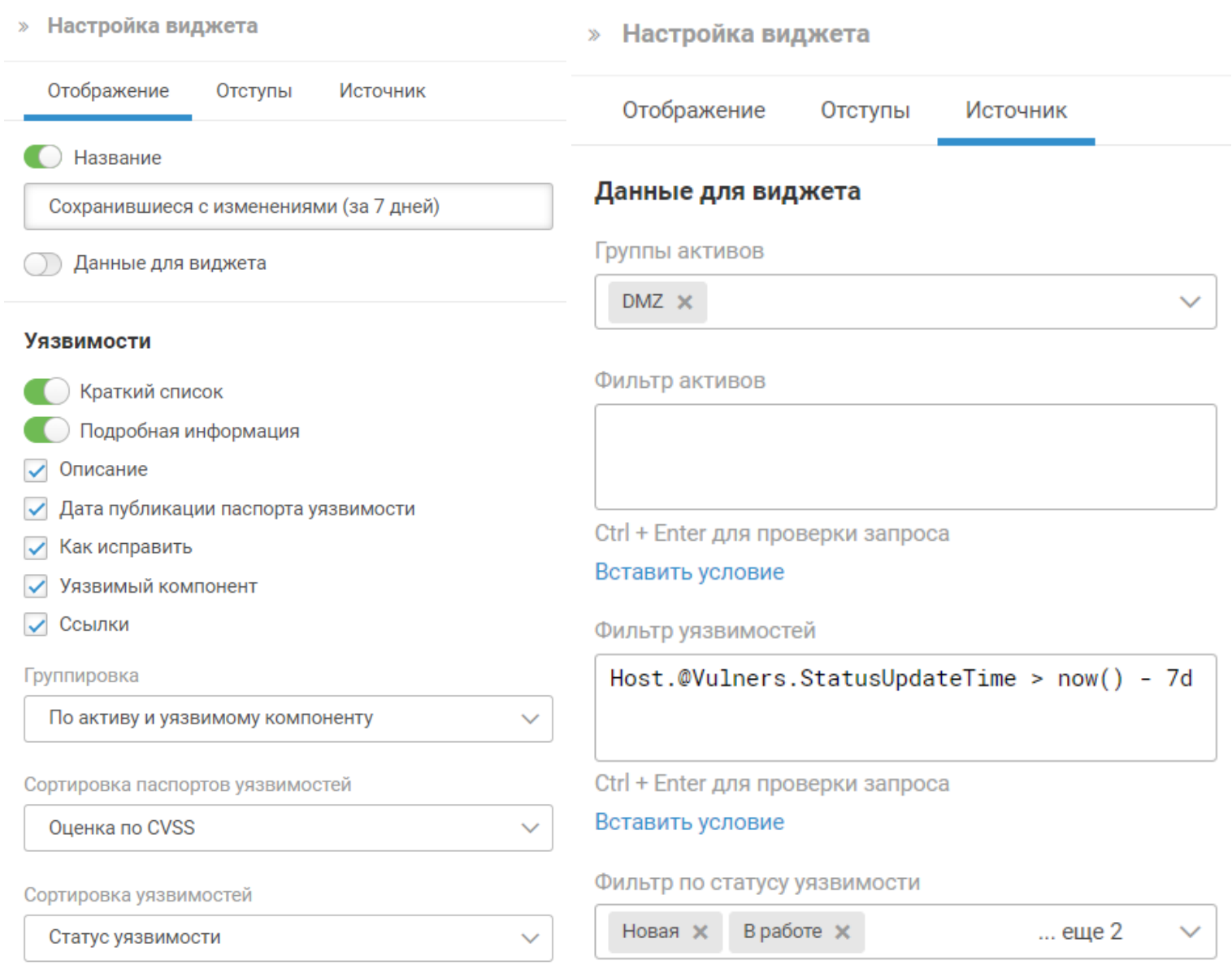
1) «Данные для виджета» -> Отключить
2) «Группировка» -> Выбираем «По активу и уязвимому компоненту»
3) «Сортировка паспортов уязвимостей» -> Выбираем «Оценка по CVSS»
4) «Сортировка уязвимостей» -> Выбираем «Статус уязвимости»

На вкладке «Источник»

1) «Группы активов» -> Указываем группу активов, по которой хотим выпустить дифференциальный отчёт, или выбираем «Все активы»
2) «Фильтр уязвимостей» -> Указываем фильтр, чтобы оставить уязвимости, статус которых обновлялся за последние 7 дней:

```
Host.@Vulners.StatusUpdateTime > now() - 7d
```

3) «Фильтр по статусу уязвимости» -> Выбираем все статусы, кроме «Исправляется», «Исключена», «Устранена»


» Настройка виджета
Отображение
Отступы
Источник
Название
Сохранившиеся с изменениями (за 7 дней)
Данные для виджета
Уязвимости
Краткий список
Подробная информация
Описание
Дата публикации паспорта уязвимости
Как исправить
Уязвимый компонент
Ссылки
Группировка
По активу и уязвимому компоненту
Сортировка паспортов уязвимостей
Оценка по CVSS
Сортировка уязвимостей
Статус уязвимости
» Настройка виджета
Отображение
Отступы
Источник
Данные для виджета
Группы активов
DMZ
Фильтр активов
Ctrl + Enter для проверки запроса
Вставить условие
Фильтр уязвимостей
Host.@Vulners.StatusUpdateTime > now() - 7d
Ctrl + Enter для проверки запроса
Вставить условие
Фильтр по статусу уязвимости
Новая
В работе
... еще 2

3. Динамика устранения конкретной уязвимости

Уязвимость CVE-2022-41076 и динамика ее устранения

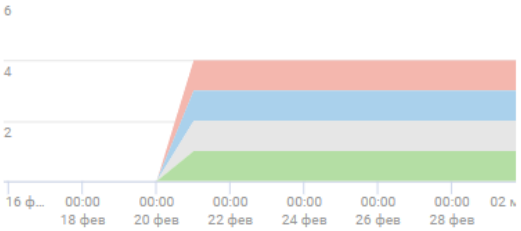
Отчет содержит список всех уязвимостей типа CVE-2022-41076 и данные о динамике их устранения за последние две недели.

Динамика устранения уязвимостей типа CVE-2022-41076 за последние две недели

2
актуальные уязвимости

1
исключена

1
устранена



Актуальные и исключенные уязвимости типа CVE-2022-41076

Уязвимость	Количество		
Удаленное выполнение кода CVE-2022-41076 Microsoft Windows	9	0	1

Удаленное выполнение кода CVE-2022-41076 Microsoft Windows

Трендовая | Удаленно | Есть исправление | 9 | 0 | 1

Уязвимость в PowerShell позволяет злоумышленникам, действующим удаленно, выполнить произвольный код и оказать воздействие на систему.

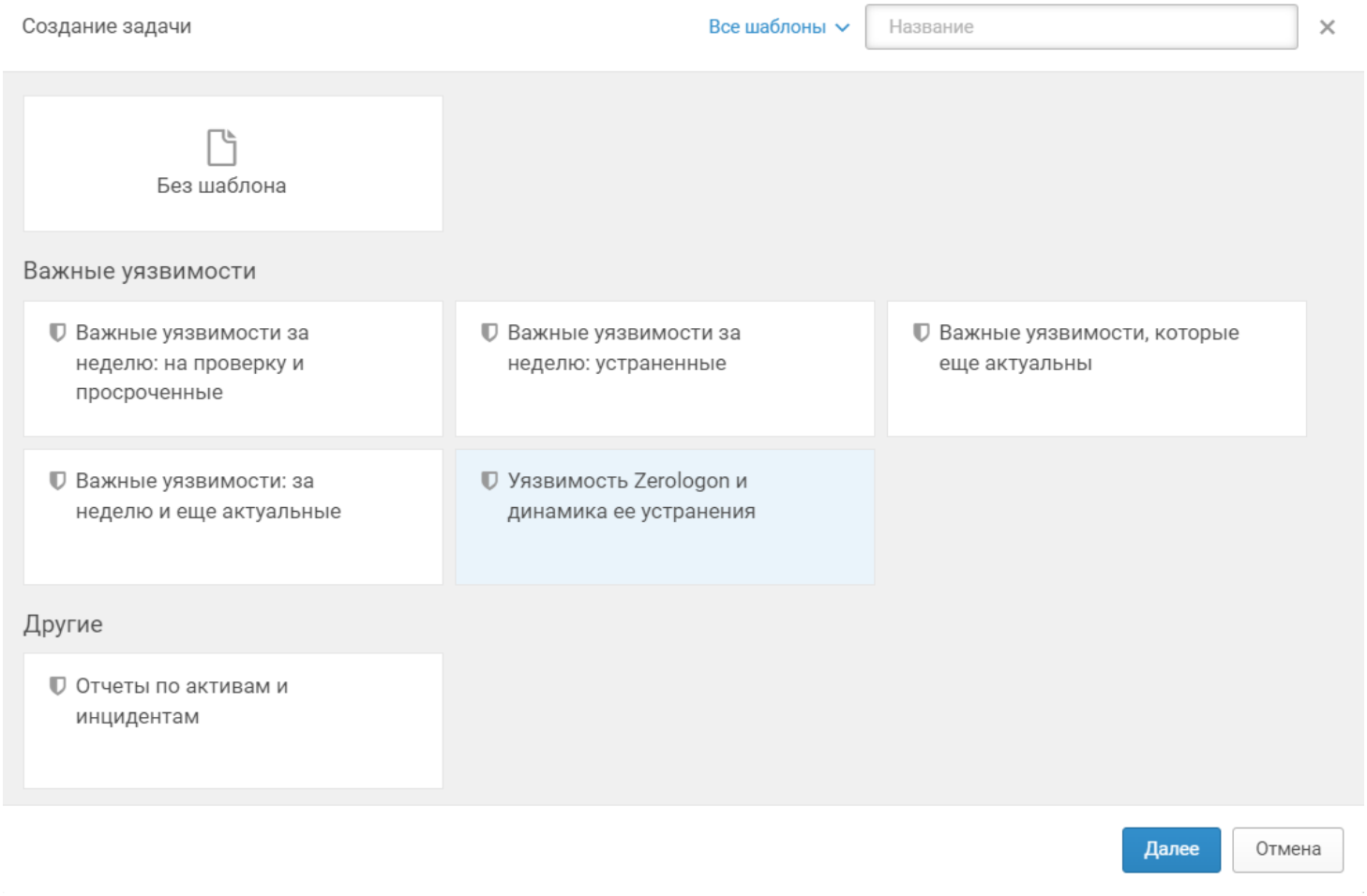
Дата публикации
13 декабря 2022, 03:00

Как исправить
Используйте рекомендации производителя:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41076

Статус	Уязвимость на активе	Обнаружена
Исключена	srv4.company.com (192.168.1.9) (Низкий риск) Важная Устранение: Плановое Microsoft Windows 6.3.9600	20 фев, 19:20
Просрочено	pc10.company.com (192.168.0.96) Важная Устранение: Плановое Microsoft Windows 6.1.7601	20 фев, 19:19
	pc13.company.com (192.168.0.99) Важная Устранение: Плановое Microsoft Windows 6.3.9600	20 фев, 19:29
	pc8.company.com (192.168.0.94) Важная Устранение: Плановое Microsoft Windows 6.1.7601	20 фев, 19:19
	pc9.company.com (192.168.0.95) Важная Устранение: Плановое Microsoft Windows 6.3.9600	20 фев, 19:19
	srv10.company.com (192.168.2.15) Важная Устранение: Плановое Microsoft Windows 6.3.9600	20 фев, 19:20
	srv13.company.com (192.168.2.8) Важная Устранение: Плановое Microsoft Windows 6.3.9600	20 фев, 19:20
	srv3.company.com (192.168.2.7) Важная Устранение: Плановое Microsoft Windows 6.3.9600	20 фев, 19:20

Шаблон: «Уязвимость Zerologon и динамика ее устранения»

Создаём новый отчёт из шаблона «Уязвимость Zerologon и динамика ее устранения».



В параметрах и текстовых блоках отчёта заменяем Zerologon на интересующую нас уязвимость, например на Bluekeep, CVE-2022-41076, BDU:2023-00755 и т. д.

« Настройка задачи

Параметры отчета | Параметры выпуска

Название

3. Уязвимость CVE-2022-41076 и динамика ее устран

Описание

Отчет содержит список уязвимостей типа CVE-2022-41076 и данные о динамике их устранения за последние две недели. На его основе вы можете создавать собственные шаблоны отчетов по другим уязвимостям, указав их CVE-идентификаторы в фильтре уязвимостей.

Внешний вид

Шрифт по умолчанию

Roboto

Верхний колонтитул

Нижний колонтитул

Настройка колонтитулов

Уязвимость CVE-2022-41076 и динамика ее устранения

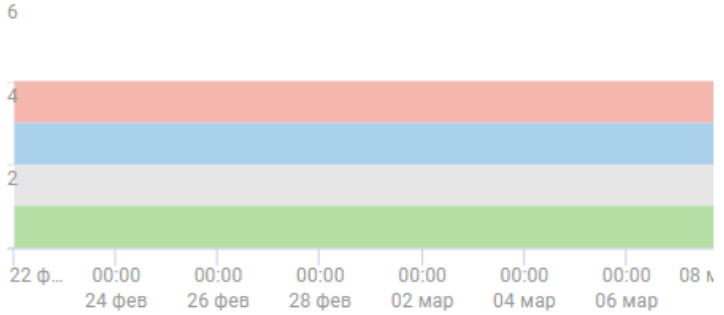
Отчет содержит список всех уязвимостей типа CVE-2022-41076 и данные о динамике их устранения за последние две недели.

Динамика устранения уязвимостей типа CVE-2022-41076 за последние две недели

2
актуальные уязвимости

1
исключена

1
устранена



Актуальные и исключенные уязвимости типа CVE-2022-41076

Уязвимость	Количество		
Удаленное выполнение кода CVE-2022-41076 Microsoft Windows	9	0	1

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

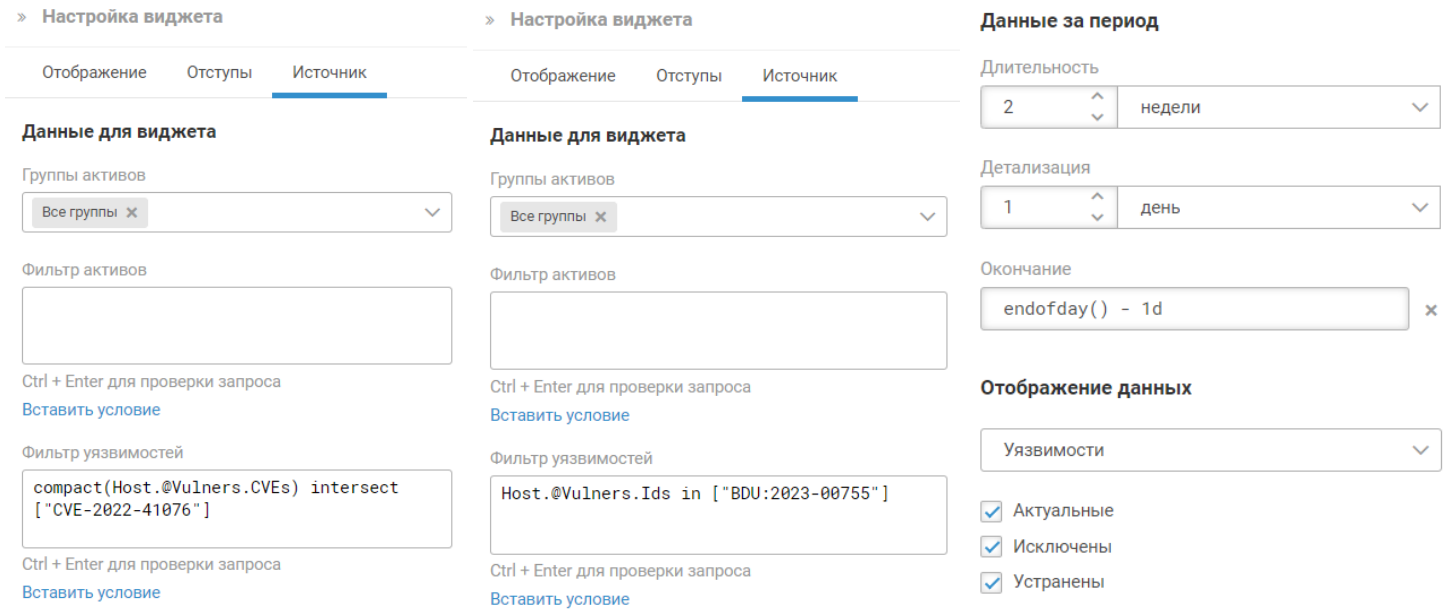
В настройках виджета «Динамика устранения уязвимостей типа … за последние две недели» указываем:

На вкладке «Источник»

1) «Группы активов» -> Указываем группу активов, по которой хотим проследить динамику устранения уязвимости, или выбираем «Все активы»
2) «Фильтр уязвимостей» -> Редактируем системный фильтр, указывая свой идентификатор уязвимости:

Для CVE	compact(Host.@Vulners.CVEs) intersect ["CVE-2022-41076"]
Для BDU, MP8ID и других	Host.@Vulners.Ids in ["BDU:2023-00755"]

3) В разделе «Данные за период» -> Задаём свой интервал, за который хотим проследить динамику устранения уязвимости, или оставляем значения по умолчанию.
4) Раздел «Отображение данных» -> Отмечаем галочкой статус «Устранены».

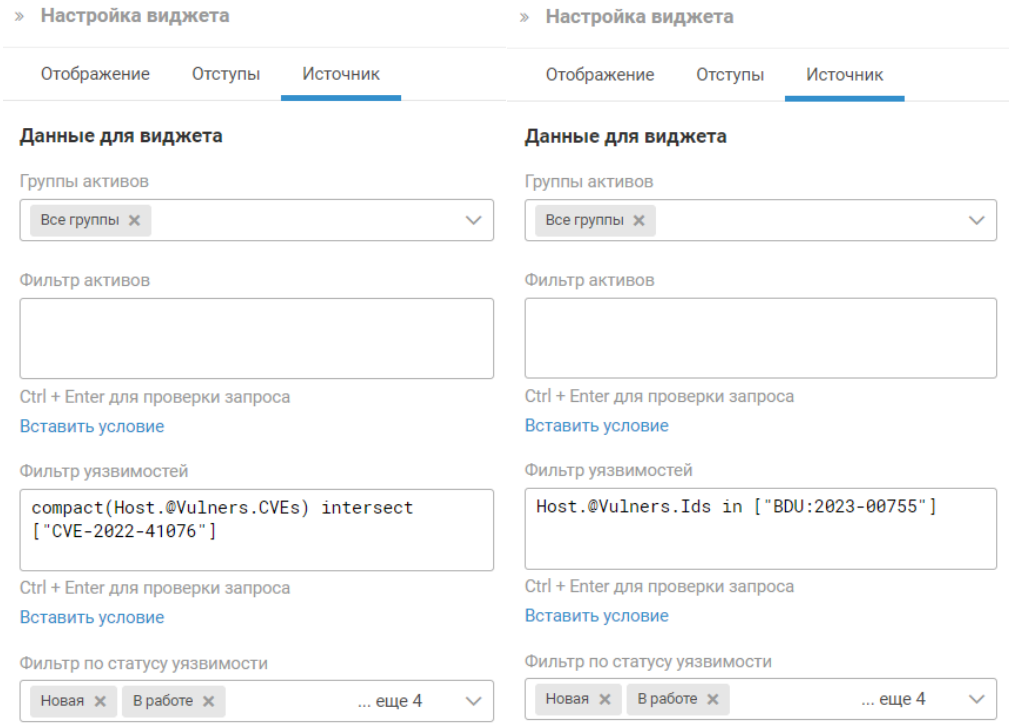


В настройках виджета «Актуальные и исключенные уязвимости типа …» указываем:

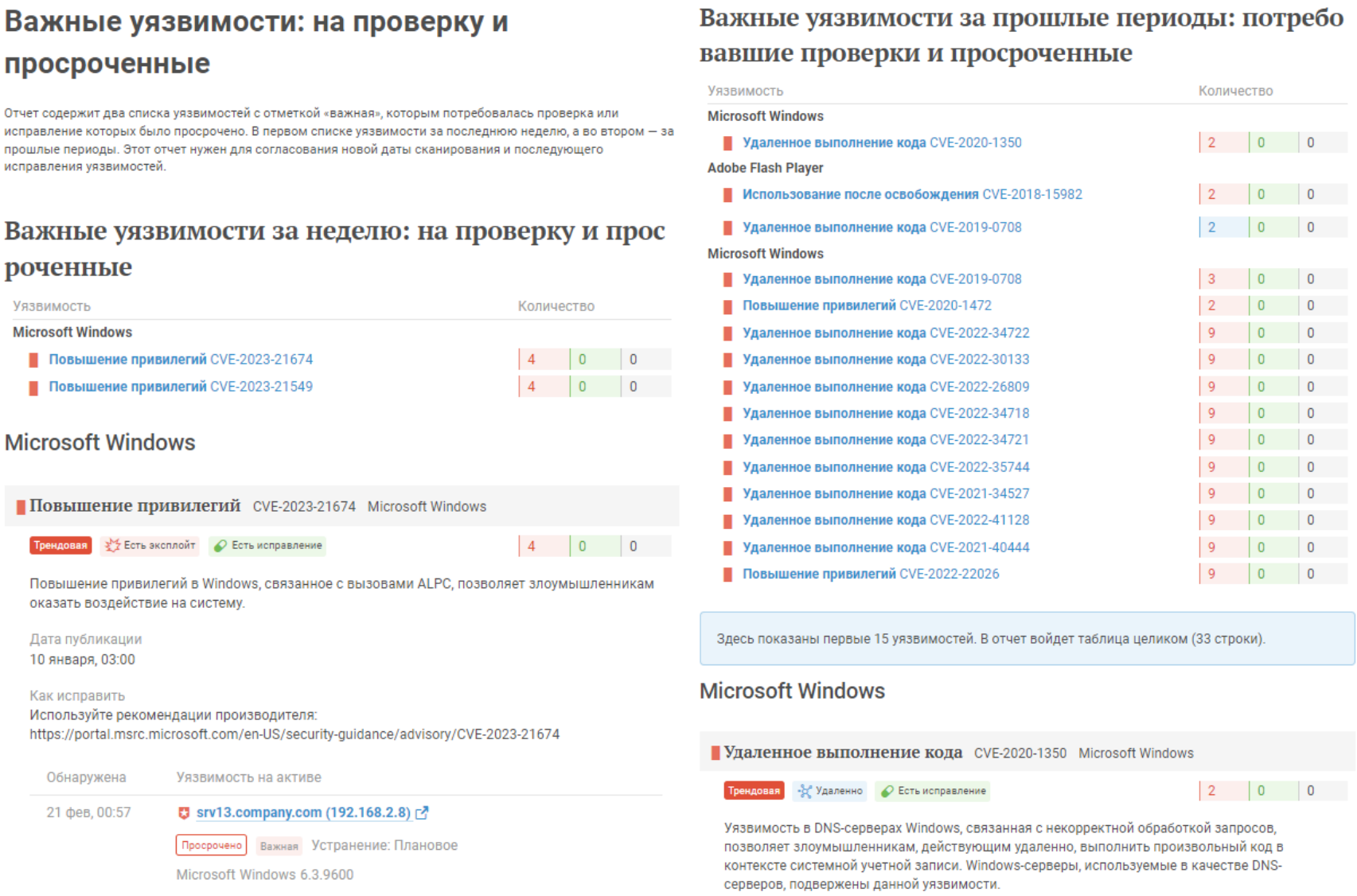
На вкладке «Источник»

1) «Группы активов» -> Указываем группу активов, по которой хотим проследить динамику устранения уязвимости, или выбираем «Все активы»
2) «Фильтр уязвимостей» -> Редактируем системный фильтр, указывая свой идентификатор уязвимости:

Для CVE	compact(Host.@Vulners.CVEs) intersect ["CVE-2022-41076"]
Для BDU, MP8ID и других	Host.@Vulners.Ids in ["BDU:2023-00755"]



4. Важные уязвимости за неделю: на проверку и просроченные



Важные уязвимости: на проверку и просроченные

Отчет содержит два списка уязвимостей с отметкой «важная», которым потребовалась проверка или исправление которых было просрочено. В первом списке уязвимости за последнюю неделю, а во втором — за прошлые периоды. Этот отчет нужен для согласования новой даты сканирования и последующего исправления уязвимостей.

Важные уязвимости за неделю: на проверку и просроченные

Уязвимость	Количество		
Microsoft Windows			
Повышение привилегий CVE-2023-21674	4	0	0
Повышение привилегий CVE-2023-21549	4	0	0

Microsoft Windows

Повышение привилегий CVE-2023-21674 Microsoft Windows

Трендовая | Есть эксплойт | Есть исправление | 4 | 0 | 0

Повышение привилегий в Windows, связанное с вызовами ALPC, позволяет злоумышленникам оказать воздействие на систему.

Дата публикации
10 января, 03:00

Как исправить
Используйте рекомендации производителя:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21674

Обнаружена	Уязвимость на активе
21 фев, 00:57	srv13.company.com (192.168.2.8) Просрочено | Важная | Устранение: Плановое Microsoft Windows 6.3.9600

Важные уязвимости за прошлые периоды: потребовавшие проверки и просроченные

Уязвимость	Количество		
Microsoft Windows			
Удаленное выполнение кода CVE-2020-1350	2	0	0
Adobe Flash Player			
Использование после освобождения CVE-2018-15982	2	0	0
Удаленное выполнение кода CVE-2019-0708	2	0	0
Microsoft Windows			
Удаленное выполнение кода CVE-2019-0708	3	0	0
Повышение привилегий CVE-2020-1472	2	0	0
Удаленное выполнение кода CVE-2022-34722	9	0	0
Удаленное выполнение кода CVE-2022-30133	9	0	0
Удаленное выполнение кода CVE-2022-26809	9	0	0
Удаленное выполнение кода CVE-2022-34718	9	0	0
Удаленное выполнение кода CVE-2022-34721	9	0	0
Удаленное выполнение кода CVE-2022-35744	9	0	0
Удаленное выполнение кода CVE-2021-34527	9	0	0
Удаленное выполнение кода CVE-2022-41128	9	0	0
Удаленное выполнение кода CVE-2021-40444	9	0	0
Повышение привилегий CVE-2022-22026	9	0	0

Здесь показаны первые 15 уязвимостей. В отчет войдет таблица целиком (33 строки).

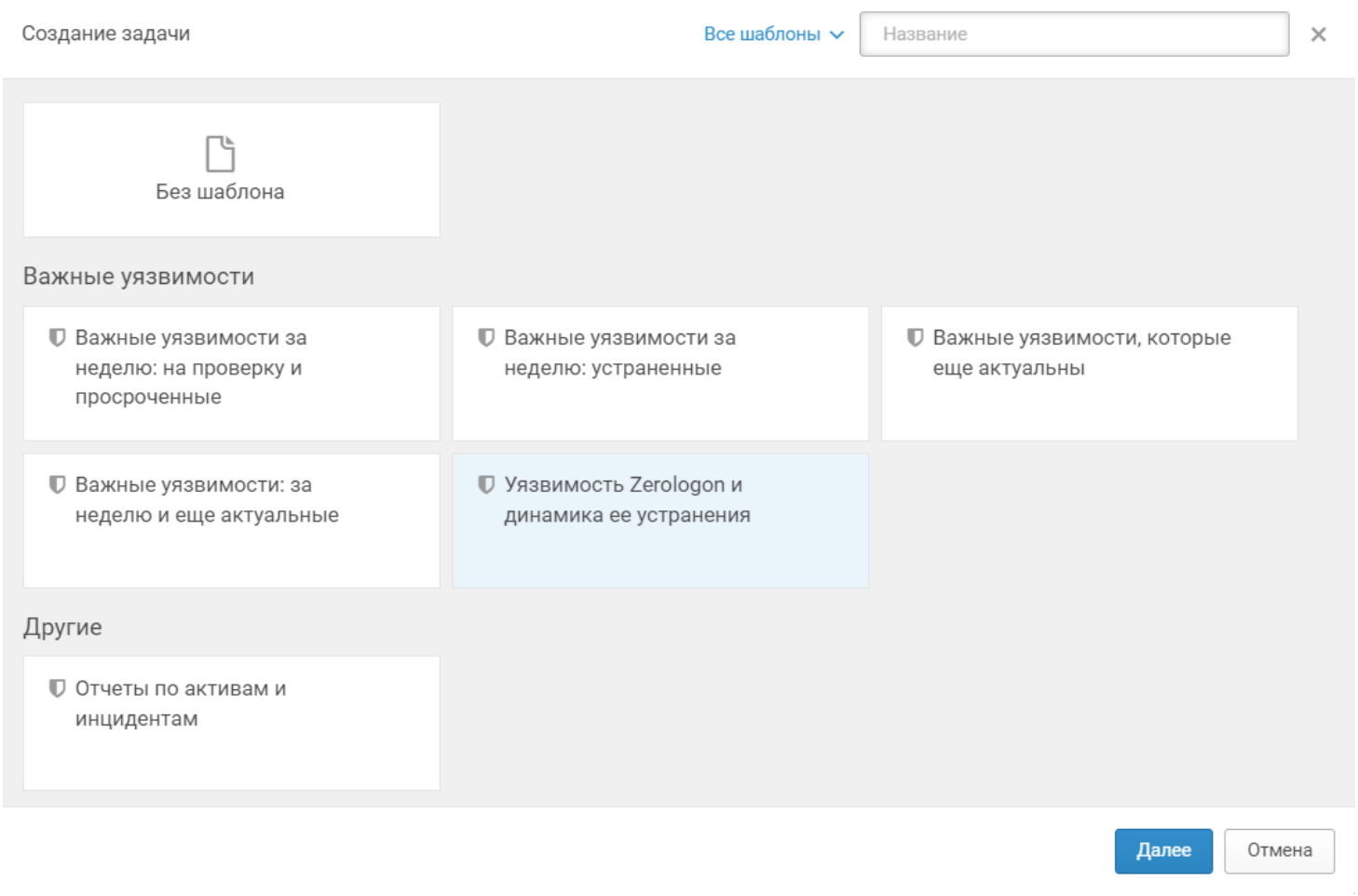
Microsoft Windows

Удаленное выполнение кода CVE-2020-1350 Microsoft Windows

Трендовая | Удаленно | Есть исправление | 2 | 0 | 0

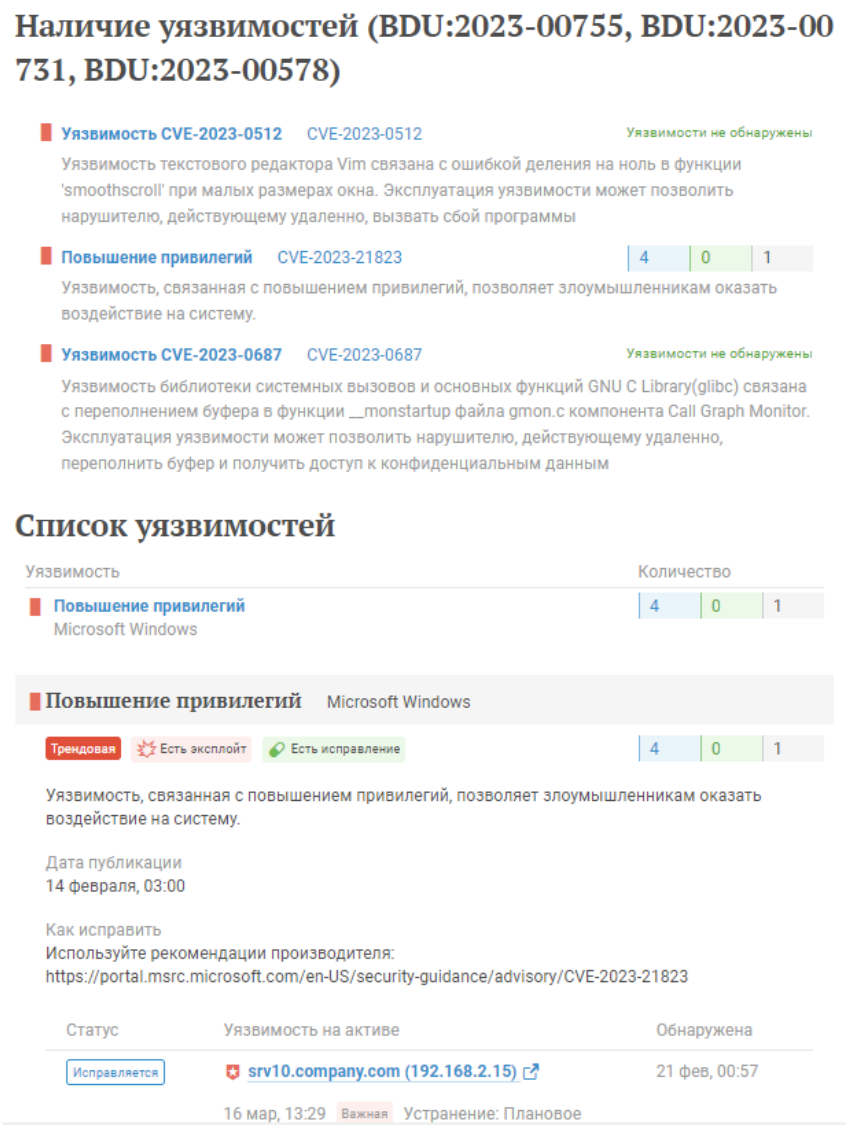
Уязвимость в DNS-серверах Windows, связанная с некорректной обработкой запросов, позволяет злоумышленникам, действующим удаленно, выполнить произвольный код в контексте системной учетной записи. Windows-серверы, используемые в качестве DNS-серверов, подвержены данной уязвимости.

Создаём новый отчёт из шаблона «Важные уязвимости за неделю: на проверку и просроченные».



Все параметры отчёта можно оставить по умолчанию.

5. Отчёт о наличии конкретных уязвимостей (CVE, BDU, …)



На вкладке «Система» -> «Отчёты» создаём новый отчёт без шаблона.

Виджет: «Наличие уязвимостей (BDU:2023-00755, BDU:2023-00731, BDU:2023-00578)»

Добавляем стандартный виджет «Трендовые уязвимости».

В настройках виджета указываем:

На вкладке «Отображение»

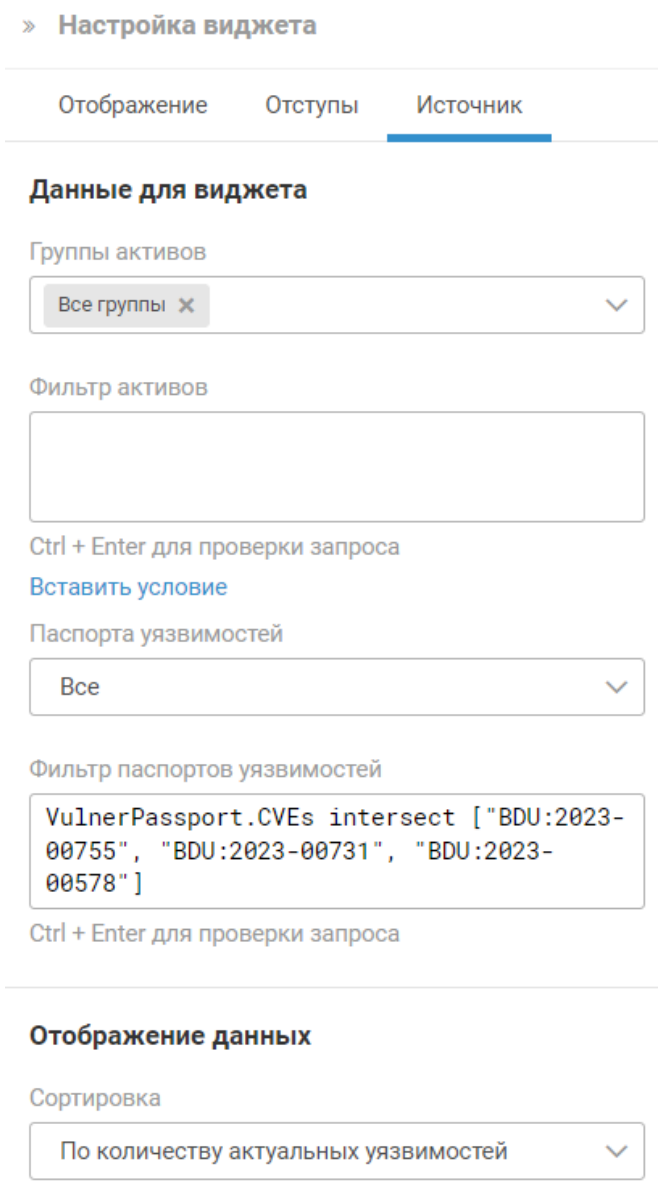
1) «Название» -> Указываем «Наличие уязвимостей (BDU:2023-00755, BDU:2023-00731, BDU:2023-00578)»
2) «Данные для виджета» -> Отключить

На вкладке «Источник»

1) «Группы активов» -> Указываем группу активов, по которой хотим выпустить отчёт о наличии уязвимостей, или выбираем «Все активы»
2) «Фильтр паспортов уязвимостей» -> Указываем фильтр, чтобы выбрать паспорта уязвимостей, наличие которых хотим проверить:

```
VulnerPassport.Ids intersect ["BDU:2023-00755", "BDU:2023-00731", "BDU:2023-00578", "CVE-2022-41076"]
```

3) «Отображение данных» -> Выбираем «По количеству актуальных уязвимостей»


» Настройка виджета
Отображение
Отступы
Источник
Данные для виджета
Группы активов
Все группы
Фильтр активов
Ctrl + Enter для проверки запроса
Вставить условие
Паспорта уязвимостей
Все
Фильтр паспортов уязвимостей
VulnerPassport.CVEs intersect ["BDU:2023-00755", "BDU:2023-00731", "BDU:2023-00578"]
Ctrl + Enter для проверки запроса
Отображение данных
Сортировка
По количеству актуальных уязвимостей

Виджет: «Список уязвимостей»

Добавляем стандартный виджет «Список уязвимостей».

В настройках виджета указываем:

На вкладке «Отображение»

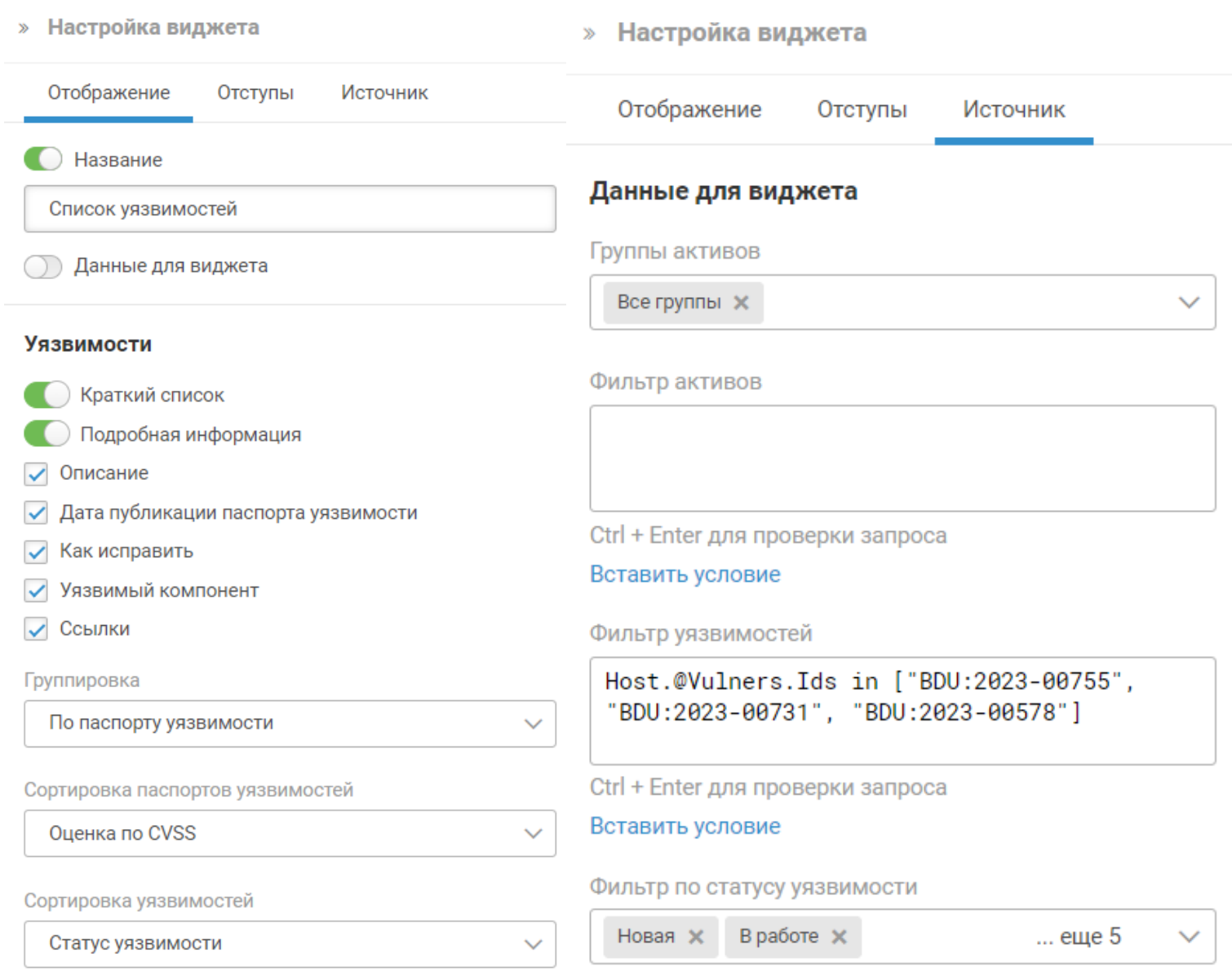
1) «Данные для виджета» -> Отключить
2) «Группировка» -> Выбираем «По паспорту уязвимости»
3) «Сортировка паспортов уязвимостей» -> Выбираем «Оценка по CVSS»
4) «Сортировка уязвимостей» -> Выбираем «Статус уязвимости»

На вкладке «Источник»

1) «Группы активов» -> Указываем группу активов, по которой хотим выпустить отчёт о наличии уязвимостей, или выбираем «Все активы»
2) «Фильтр уязвимостей» -> Указываем фильтр, чтобы выбрать экземпляры уязвимостей, наличие которых хотим проверить:

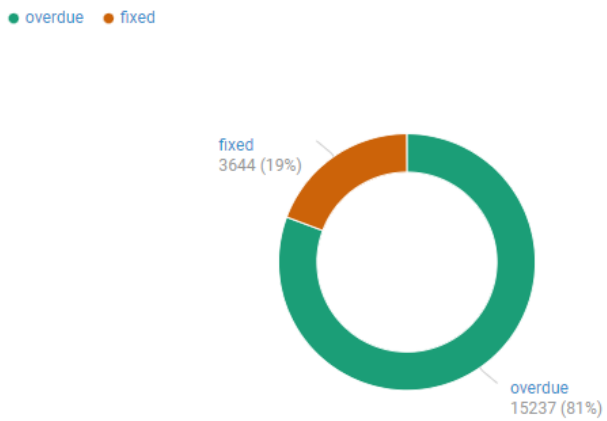
```
Host.@Vulners.Ids in ["BDU:2023-00755", "BDU:2023-00731", "BDU:2023-00578", "CVE-2022-41076"]
```

3) «Фильтр по статусу уязвимости» -> Выбираем все статусы

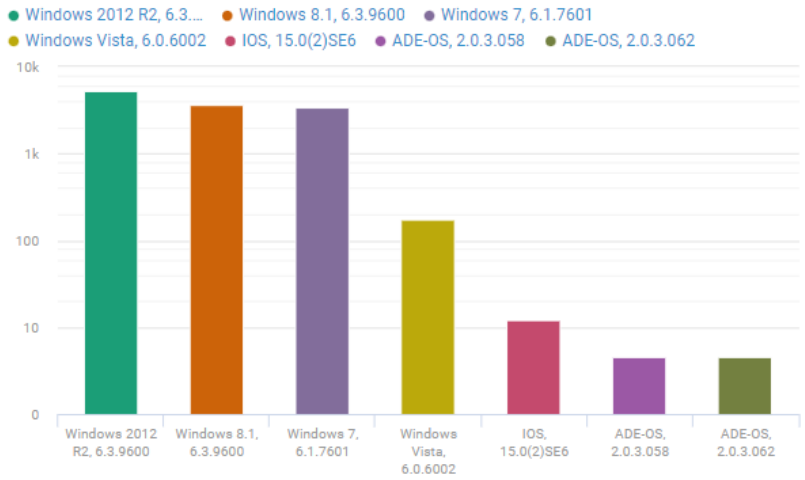

» Настройка виджета
Отображение
Отступы
Источник
Название
Список уязвимостей
Данные для виджета
Уязвимости
Краткий список
Подробная информация
Описание
Дата публикации паспорта уязвимости
Как исправить
Уязвимый компонент
Ссылки
Группировка
По паспорту уязвимости
Сортировка паспортов уязвимостей
Оценка по CVSS
Сортировка уязвимостей
Статус уязвимости
» Настройка виджета
Отображение
Отступы
Источник
Данные для виджета
Группы активов
Все группы
Фильтр активов
Ctrl + Enter для проверки запроса
Вставить условие
Фильтр уязвимостей
Host.@Vulners.Ids in ["BDU:2023-00755", "BDU:2023-00731", "BDU:2023-00578"]
Ctrl + Enter для проверки запроса
Вставить условие
Фильтр по статусу уязвимости
Новая
В работе
... еще 5

6. Отчёт о сбоях в процессе патч-менеджмента IT

Уязвимости: Просроченные | Устранённые



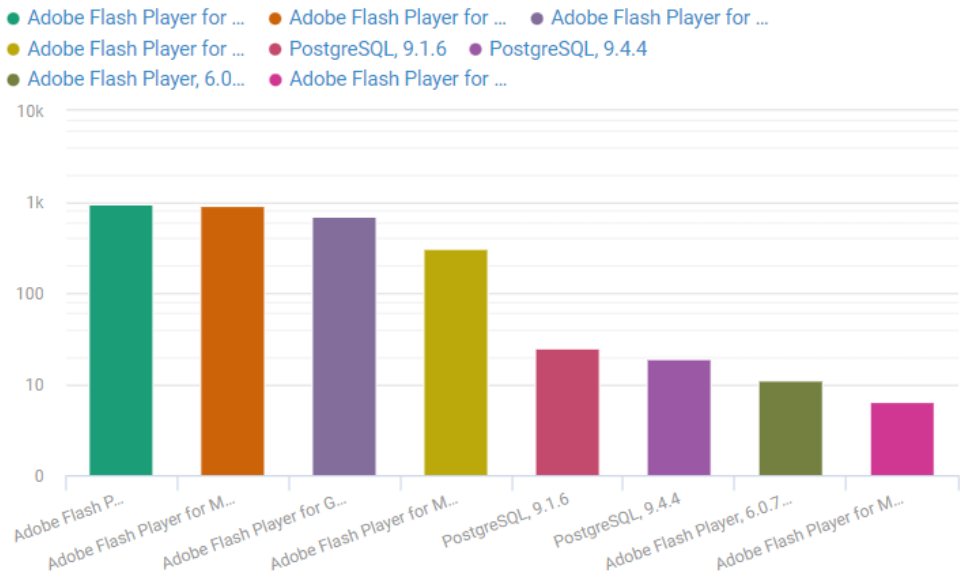
(П) Уязвимости ОС на активах



(П) Уязвимости ОС на активах (по хосту)

Хост, ОС, Версия	Кол-во уязвимостей
srv13.company.com (192.168.2.8) Windows 2012 R2 6.3.9600	1982
pc9.company.com (192.168.0.95) Windows 8.1 6.3.9600	1867
pc10.company.com (192.168.0.96) Windows 7 6.1.7601	1816
pc13.company.com (192.168.0.99) Windows 8.1 6.3.9600	1742
srv10.company.com (192.168.2.15) Windows 2012 R2 6.3.9600	1732
pc8.company.com (192.168.0.94) Windows 7 6.1.7601	1525
srv6.company.com (192.168.0.11) Windows 2012 R2 6.3.9600	765
srv3.company.com (192.168.2.7) Windows 2012 R2 6.3.9600	749
pc6.company.com (192.168.0.92) Windows Vista 6.0.6002	176
switch3.company.com (192.168.0.233) IOS 15.0(2)SE6	12
aaa1 (192.168.0.248) ADE-OS 2.0.3.058	4
aaa2 (192.168.0.247) ADE-OS 2.0.3.062	4
Всего: 12	

(П) Уязвимости ПО на активах



(П) Уязвимости ПО на активах (по хостам)

Источник	Активы
Период обновления	на текущий момент
Группы активов	Все группы
Фильтр	(П) Уязвимости ПО на активах (по хостам)

@Host, Host.Softs.Name, Host.Softs.Version	Кол-во уязвимостей
pc13.company.com (192.168.0.99) Adobe Flash Player for Microsoft Edge and Internet Explorer 19.0.0.185	932
pc12.company.com (192.168.0.98) Adobe Flash Player for Microsoft Edge and Internet Explorer 19.0.0.207	892
pc8.company.com (192.168.0.94) Adobe Flash Player for Google Chrome 20.0.0.306	682
srv13.company.com (192.168.2.8) Adobe Flash Player for Microsoft Edge and Internet Explorer 11.8.800.175	156
pc9.company.com (192.168.0.95) Adobe Flash Player for Microsoft Edge and Internet Explorer 11.8.800.175	156
srv12.company.com (192.168.0.17) PostgreSQL 9.1.6	25
srv6.company.com (192.168.0.11) PostgreSQL 9.4.4	19
pc3.company.com (192.168.0.76) Adobe Flash Player 6.0.79.0	11
pc14.company.com (192.168.0.100) Adobe Flash Player for Microsoft Edge and Internet Explorer 32.0.0.255	6
Всего: 9	

(П) Уязвимости Linux пакетов на активах

Нет данных

(П) Уязвимости Linux пакетов на активах (по хостам)

Нет данных

(П) Уязвимости сетевых служб на активах

Нет данных

(П) Уязвимости сетевых служб на активах (по хостам)

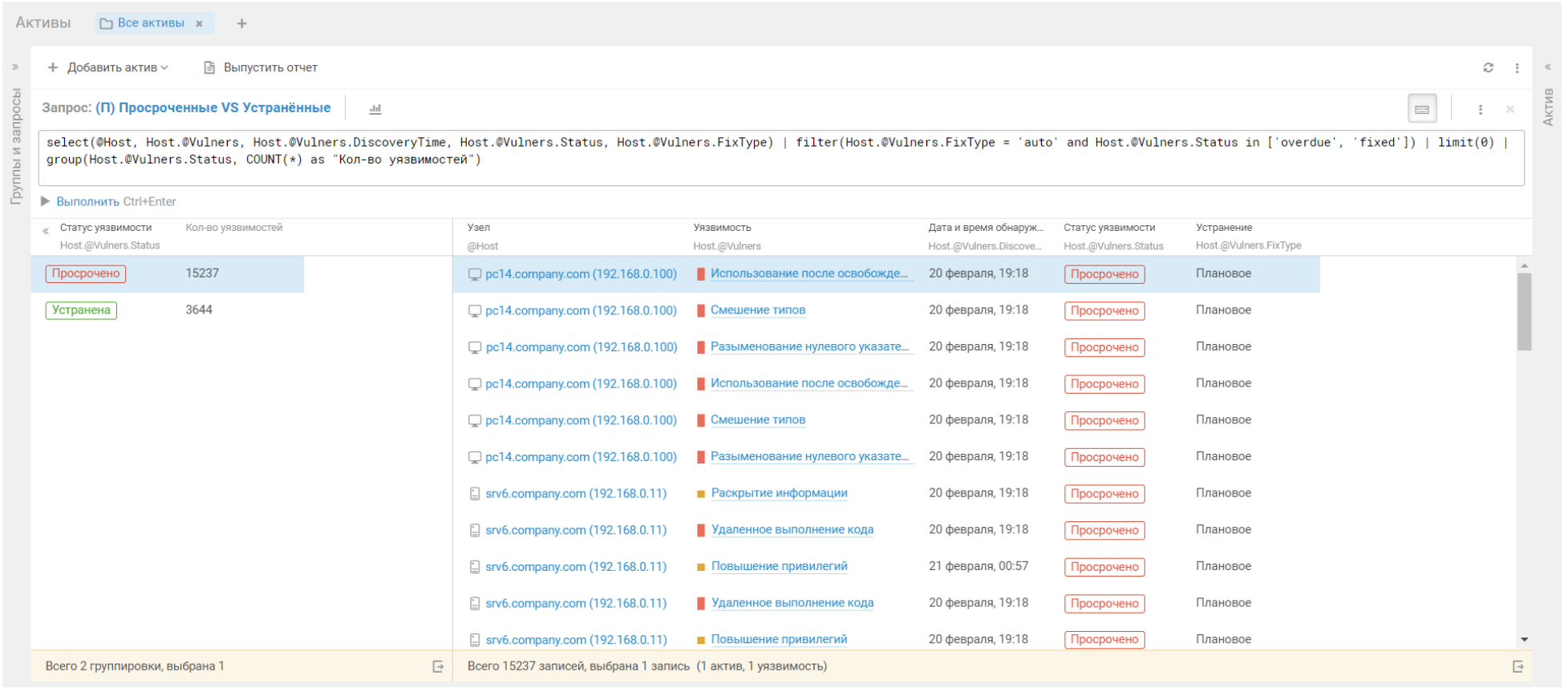
Нет данных

Виджет: «Уязвимости: Просроченные | Устранённые»

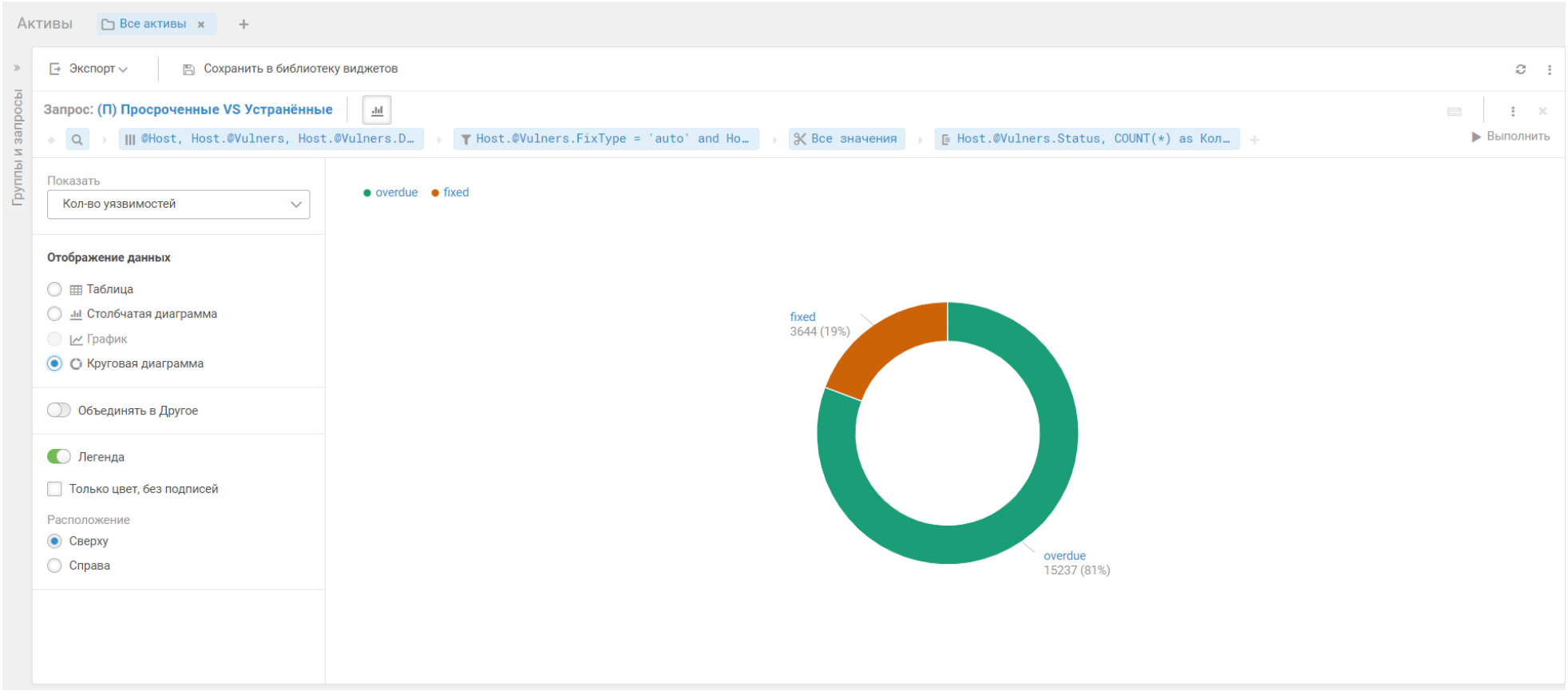
Переходим на вкладку «Активы» и нажимаем на иконку клавиатуры, чтобы перейти к текстовому редактированию запроса.

Вставляем и выполняем следующий запрос:

select(@Host, Host.@Vulners, Host.@Vulners.DiscoveryTime, Host.@Vulners.Status, Host.@Vulners.FixType) | filter(Host.@Vulners.FixType = 'auto' and Host.@Vulners.Status in ['overdue', 'fixed']) | limit(0) | group(Host.@Vulners.Status, COUNT(*) as "Кол-во уязвимостей")



Переходим в режим создания виджета нажатием соответствующей иконки:



В разделе «Отображение данных» выбираем «Круговая диаграмма».

Сохраняем получившийся виджет в библиотеку виджетов нажатием соответствующей кнопки.

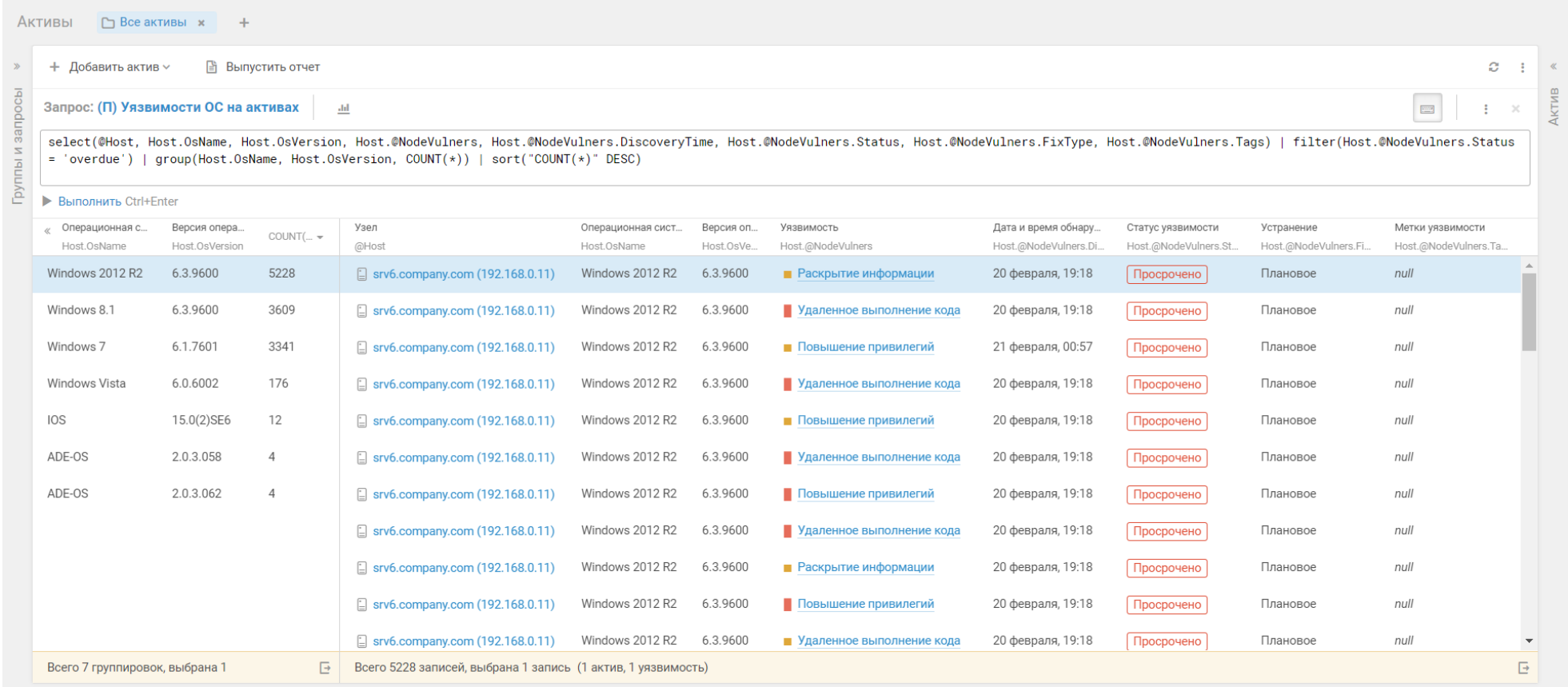
На вкладке «Система» -> «Отчёты» создаём новый отчёт без шаблона и добавляем виджет.

Виджет: «(П) Уязвимости ОС на активах»

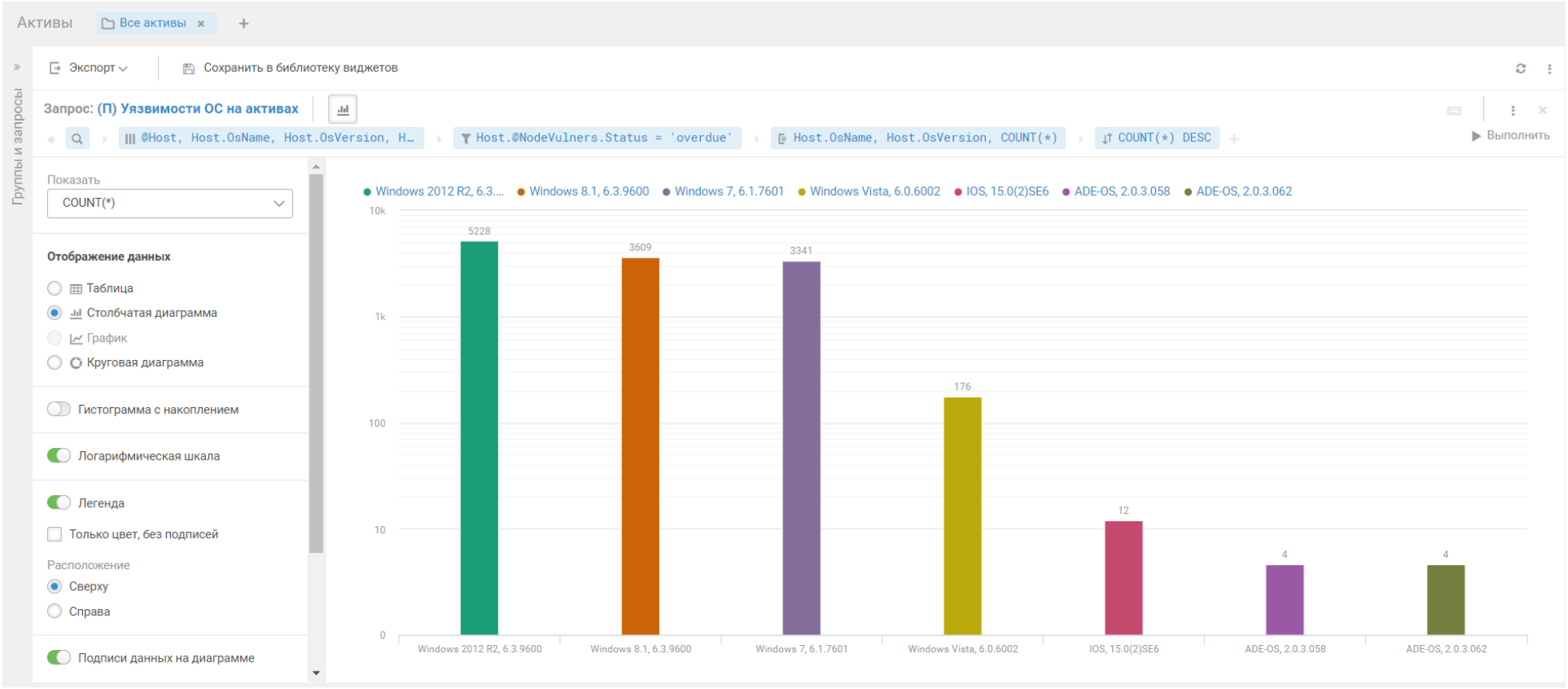
Переходим на вкладку «Активы» и нажимаем на иконку клавиатуры, чтобы перейти к текстовому редактированию запроса.

Вставляем и выполняем следующий запрос:

select(@Host, Host.OsName, Host.OsVersion, Host.@NodeVulners, Host.@NodeVulners.DiscoveryTime, Host.@NodeVulners.Status, Host.@NodeVulners.FixType, Host.@NodeVulners.Tags) | filter(Host.@NodeVulners.Status = 'overdue') | group(Host.OsName, Host.OsVersion, COUNT(*)) | sort("COUNT(*)" DESC)



Переходим в режим создания виджета нажатием соответствующей иконки:



В разделе «Отображение данных» выбираем «Столбчатая диаграмма».

Включаем использование «Логарифмической шкалы» и «Подписи данных на диаграмме».

Сохраняем получившийся виджет в библиотеку виджетов нажатием соответствующей кнопки.

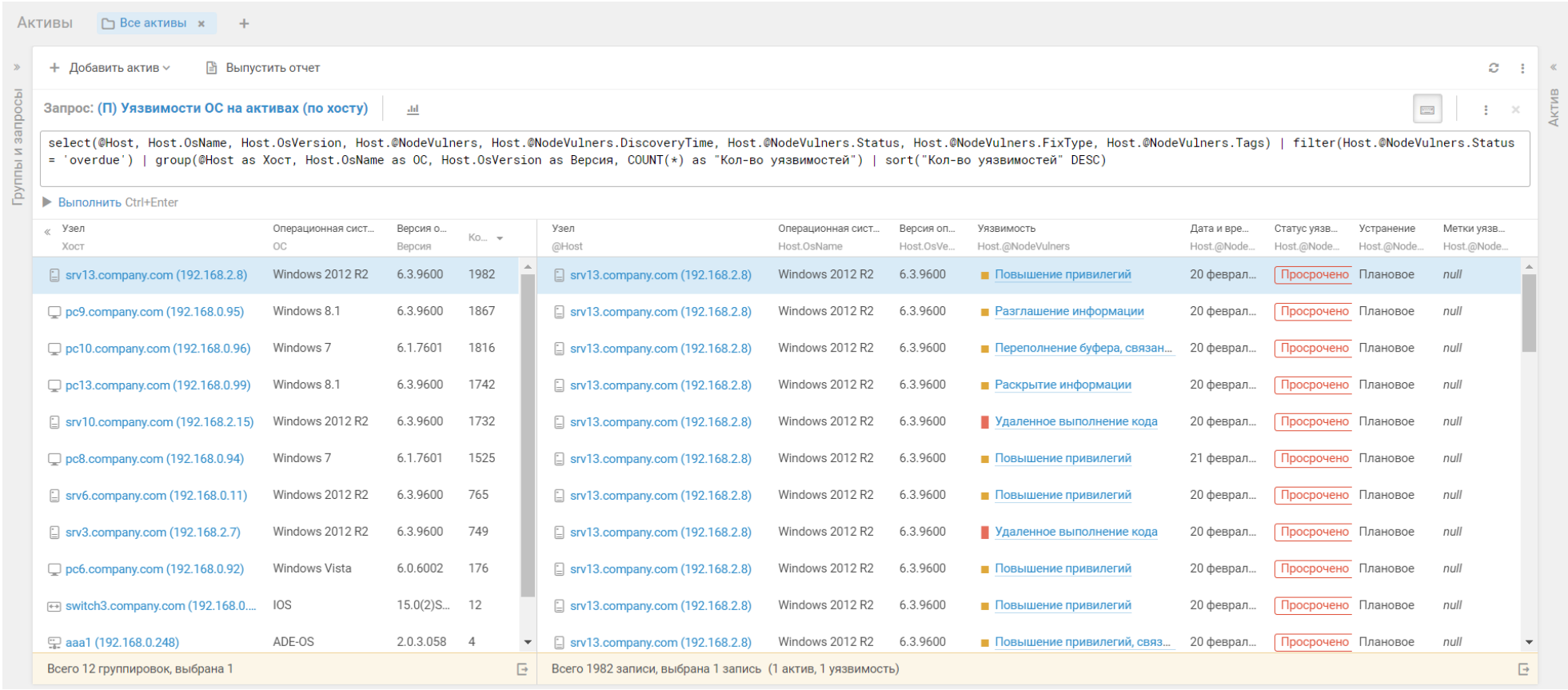
На вкладке «Система» -> «Отчёты» выбираем созданный ранее отчёт без шаблона и добавляем виджет.

Виджет: «(П) Уязвимости ОС на активах (по хосту)»

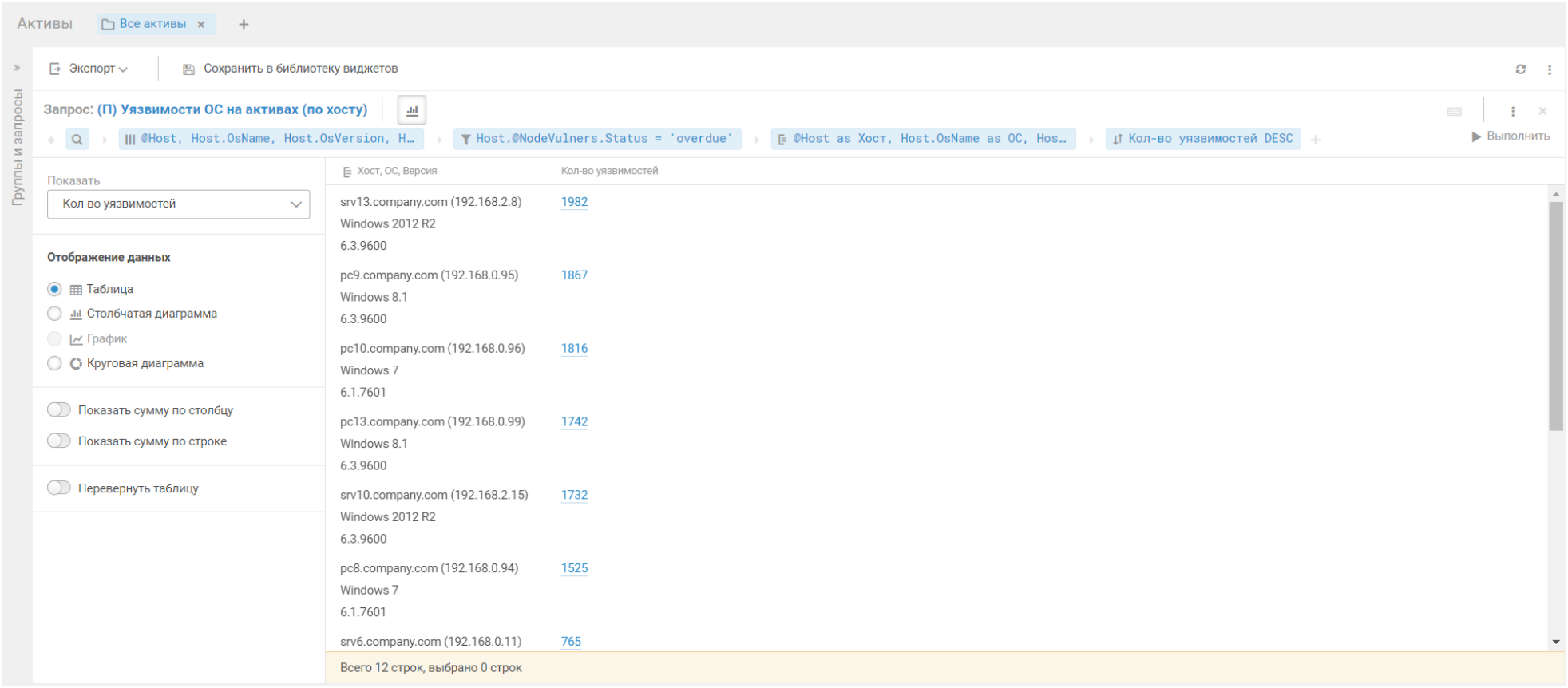
Переходим на вкладку «Активы» и нажимаем на иконку клавиатуры, чтобы перейти к текстовому редактированию запроса.

Вставляем и выполняем следующий запрос:

select(@Host, Host.OsName, Host.OsVersion, Host.@NodeVulners, Host.@NodeVulners.DiscoveryTime, Host.@NodeVulners.Status, Host.@NodeVulners.FixType, Host.@NodeVulners.Tags) | filter(Host.@NodeVulners.Status = 'overdue') | group(@Host as Хост, Host.OsName as ОС, Host.OsVersion as Версия, COUNT(*) as "Кол-во уязвимостей") | sort("Кол-во уязвимостей" DESC)



Переходим в режим создания виджета нажатием соответствующей иконки:



Сохраняем получившийся виджет в библиотеку виджетов нажатием соответствующей кнопки.

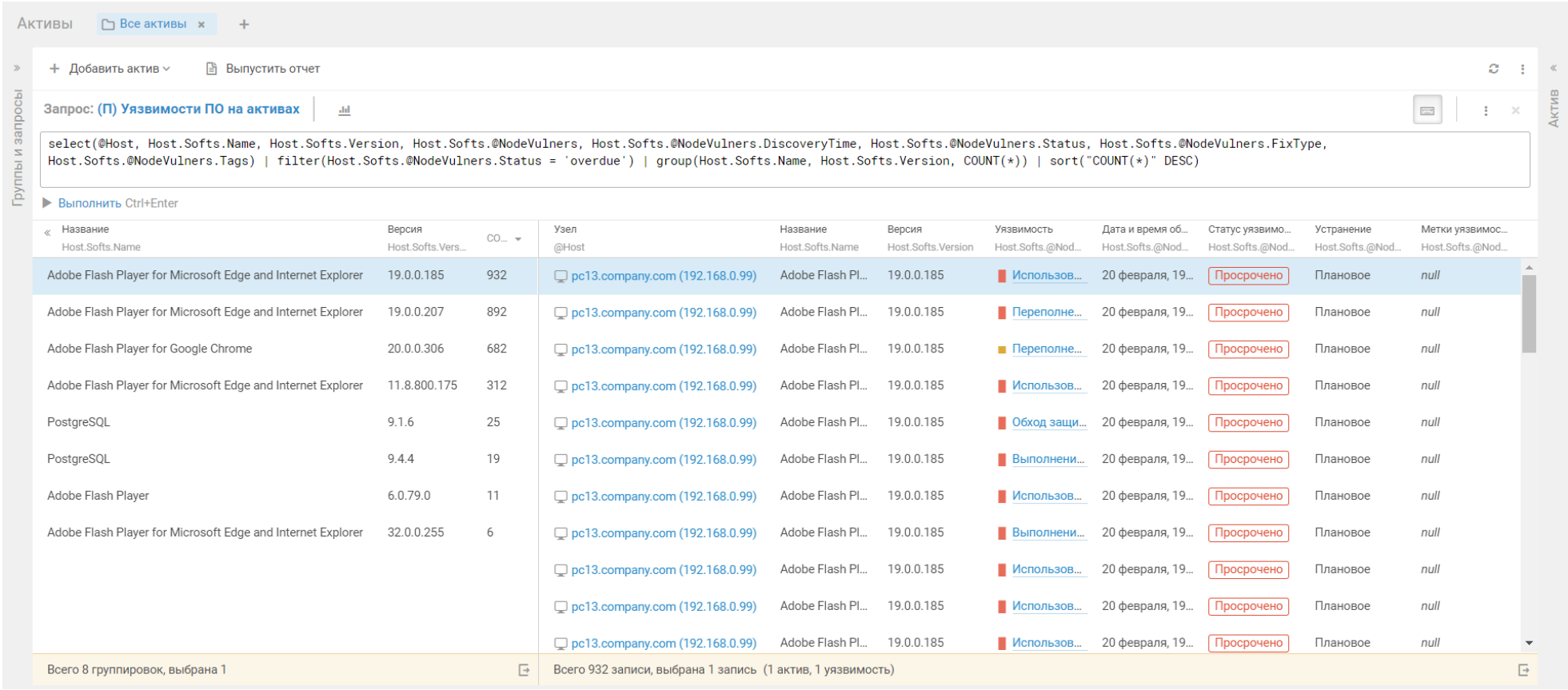
На вкладке «Система» -> «Отчёты» выбираем созданный ранее отчёт без шаблона и добавляем виджет.

Виджет: «(П) Уязвимости ПО на активах»

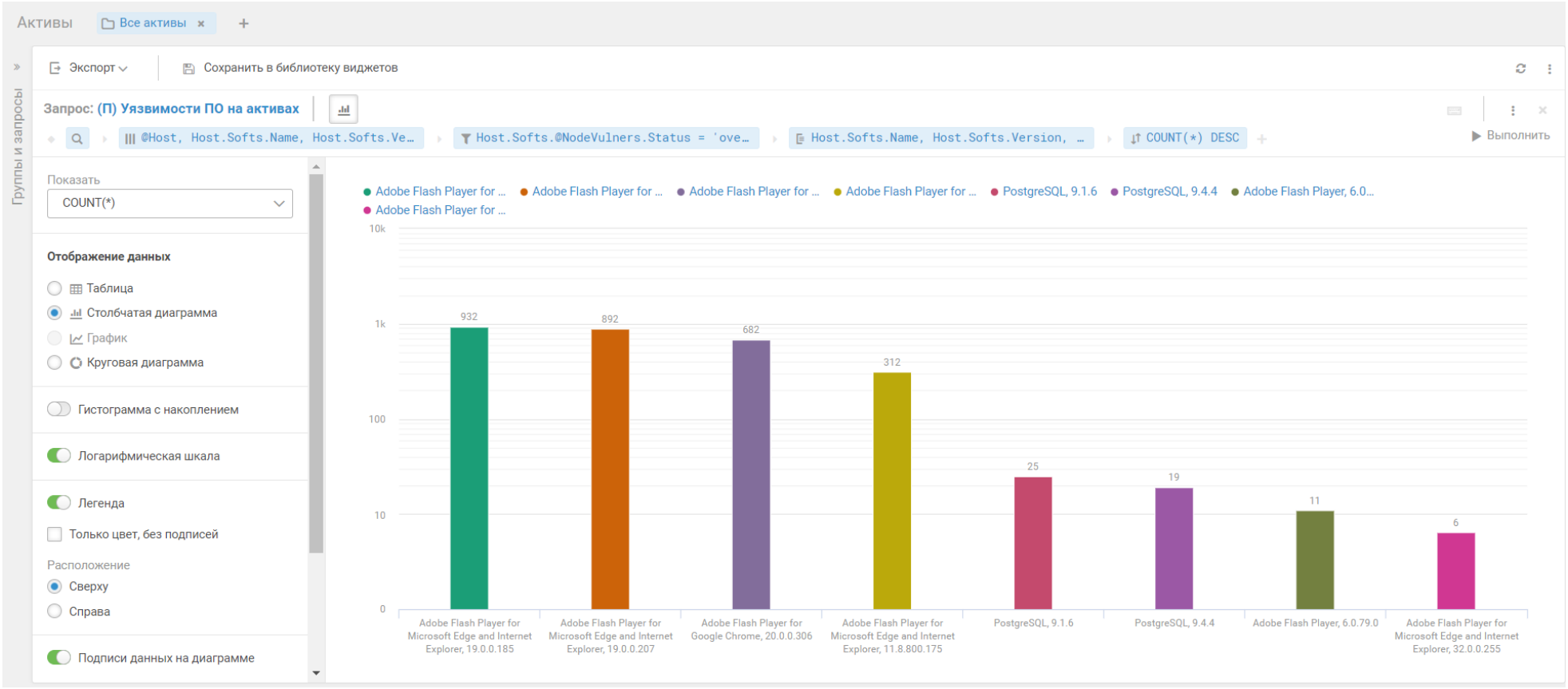
Переходим на вкладку «Активы» и нажимаем на иконку клавиатуры, чтобы перейти к текстовому редактированию запроса.

Вставляем и выполняем следующий запрос:

select(@Host, Host.Softs.Name, Host.Softs.Version, Host.Softs.@NodeVulners, Host.Softs.@NodeVulners.DiscoveryTime, Host.Softs.@NodeVulners.Status, Host.Softs.@NodeVulners.FixType, Host.Softs.@NodeVulners.Tags) | filter(Host.Softs.@NodeVulners.Status = 'overdue') | group(Host.Softs.Name, Host.Softs.Version, COUNT(*)) | sort("COUNT(*)" DESC)



Переходим в режим создания виджета нажатием соответствующей иконки:



В разделе «Отображение данных» выбираем «Столбчатая диаграмма».

Включаем использование «Логарифмической шкалы» и «Подписи данных на диаграмме».

Сохраняем получившийся виджет в библиотеку виджетов нажатием соответствующей кнопки.

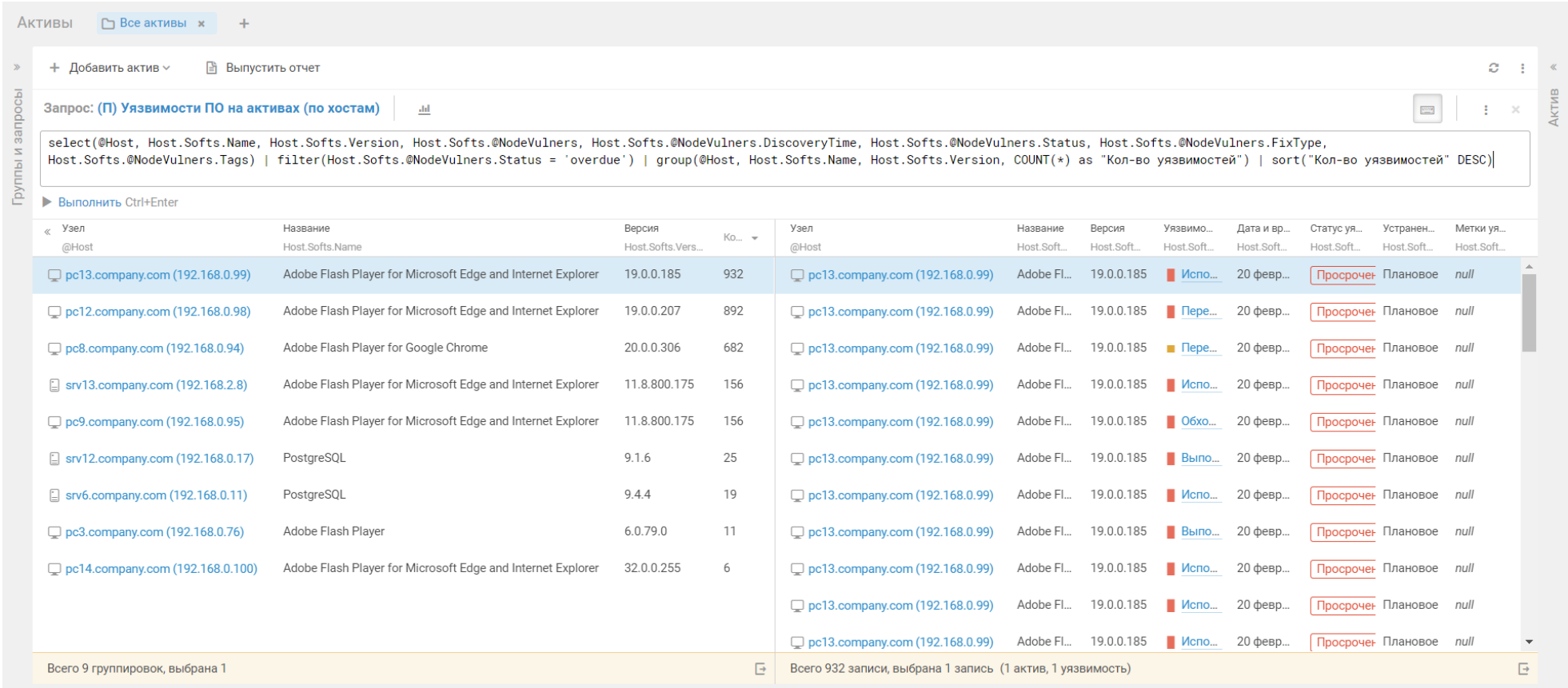
На вкладке «Система» -> «Отчёты» выбираем созданный ранее отчёт без шаблона и добавляем виджет.

Виджет: «(П) Уязвимости ПО на активах (по хостам)»

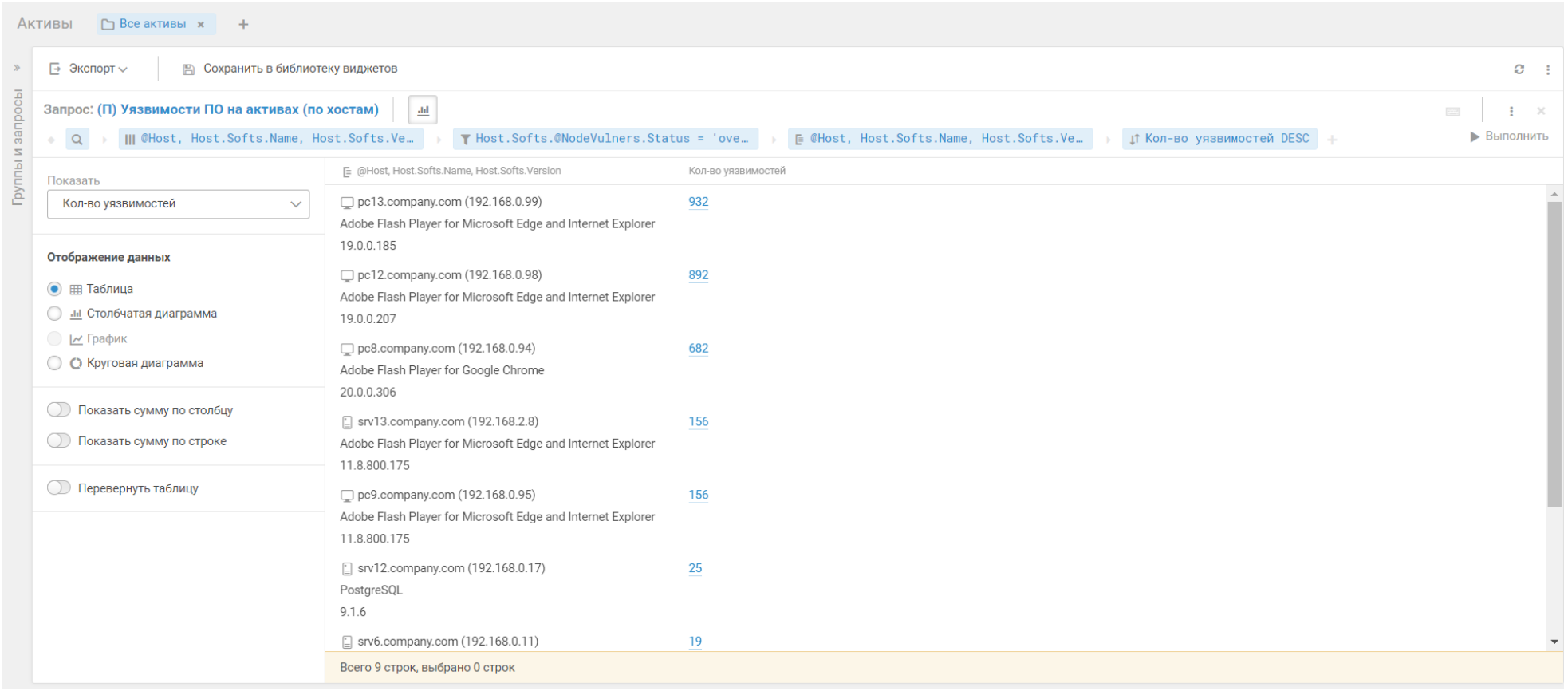
Переходим на вкладку «Активы» и нажимаем на иконку клавиатуры, чтобы перейти к текстовому редактированию запроса.

Вставляем и выполняем следующий запрос:

select(@Host, Host.Softs.Name, Host.Softs.Version, Host.Softs.@NodeVulners, Host.Softs.@NodeVulners.DiscoveryTime, Host.Softs.@NodeVulners.Status, Host.Softs.@NodeVulners.FixType, Host.Softs.@NodeVulners.Tags) | filter(Host.Softs.@NodeVulners.Status = 'overdue') | group(@Host, Host.Softs.Name, Host.Softs.Version, COUNT(*) as "Кол-во уязвимостей") | sort("Кол-во уязвимостей" DESC)



Переходим в режим создания виджета нажатием соответствующей иконки:



Сохраняем получившийся виджет в библиотеку виджетов нажатием соответствующей кнопки.

На вкладке «Система» -> «Отчёты» выбираем созданный ранее отчёт без шаблона и добавляем виджет.

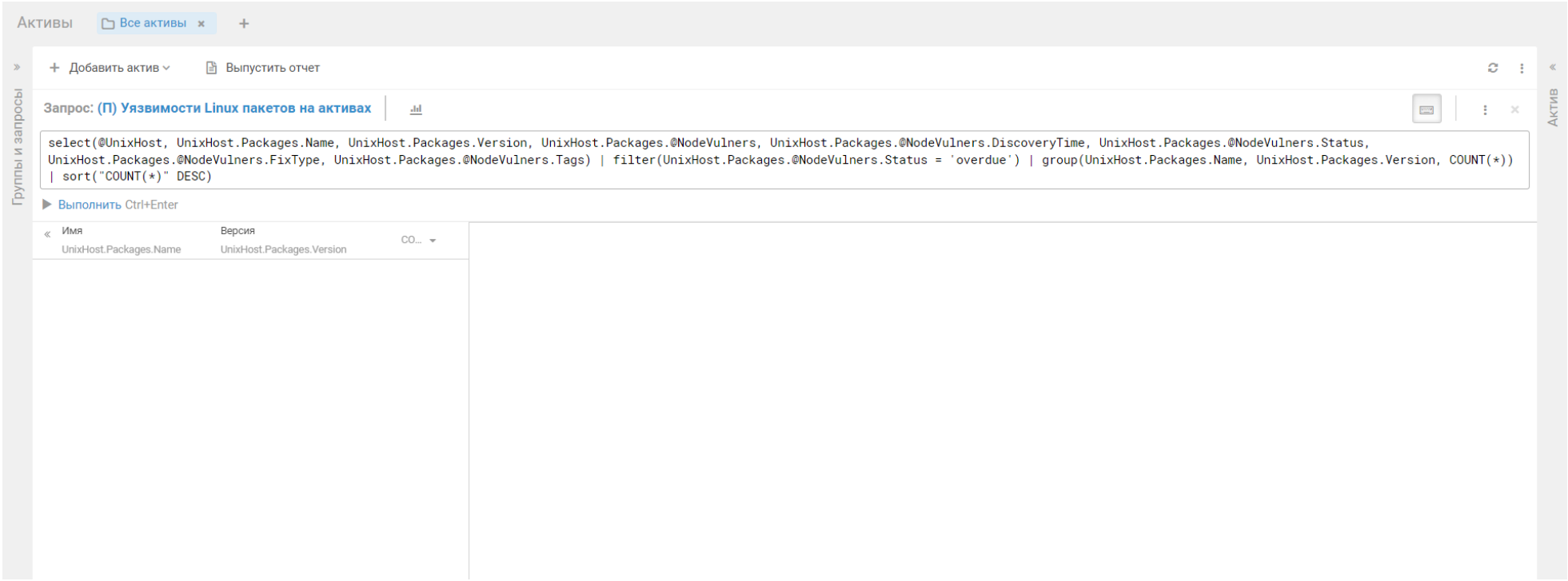
Виджет: «(П) Уязвимости Linux пакетов на активах»

Переходим на вкладку «Активы» и нажимаем на иконку клавиатуры, чтобы перейти к текстовому редактированию запроса.

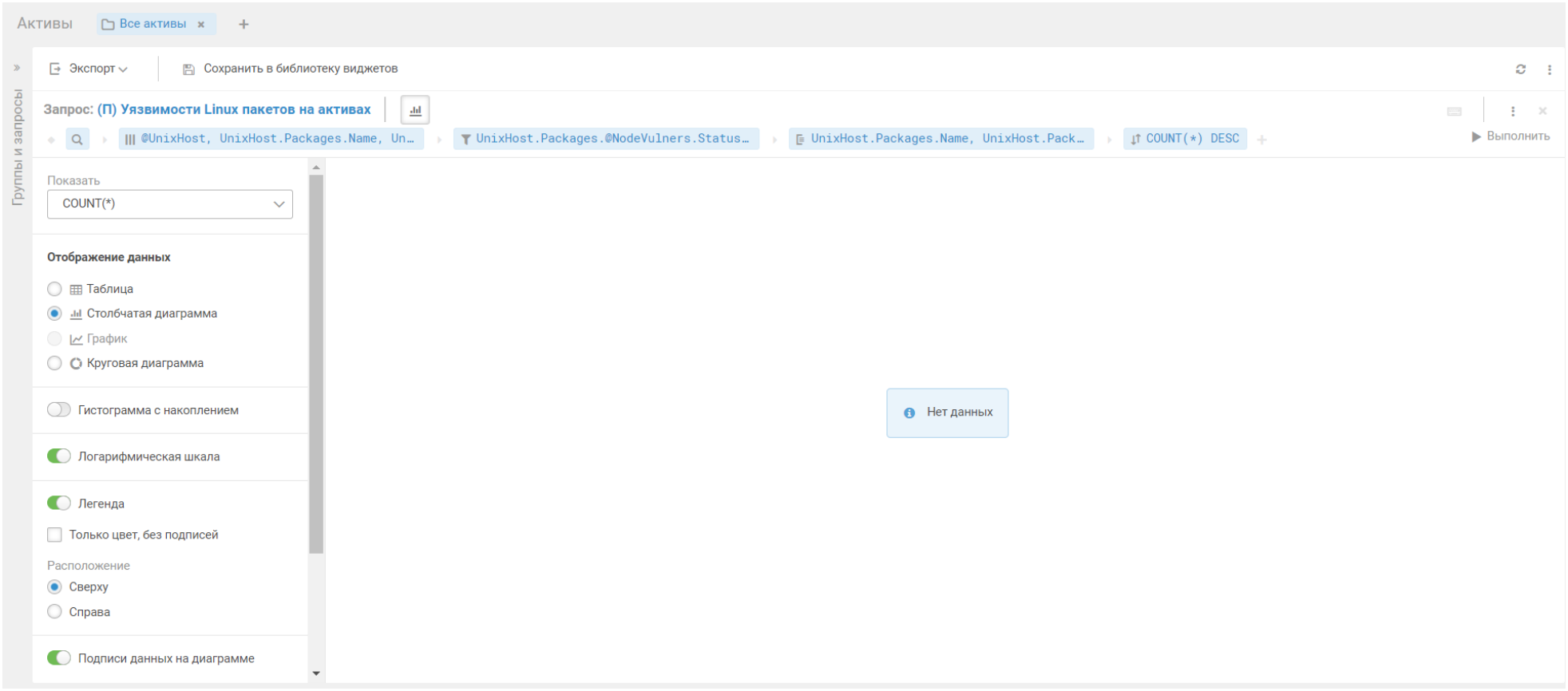
Вставляем и выполняем следующий запрос:

select(@UnixHost, UnixHost.Packages.Name, UnixHost.Packages.Version, UnixHost.Packages.@NodeVulners, UnixHost.Packages.@NodeVulners.DiscoveryTime, UnixHost.Packages.@NodeVulners.Status, UnixHost.Packages.@NodeVulners.FixType, UnixHost.Packages.@NodeVulners.Tags) | filter(UnixHost.Packages.@NodeVulners.Status = 'overdue') | group(UnixHost.Packages.Name, UnixHost.Packages.Version, COUNT(*)) | sort("COUNT(*)" DESC)

*Если в результате выполнения запроса получилась пустая таблица, нарушения регламентов патч-менеджмента IT по данному типу уязвимостей отсутствуют



Переходим в режим создания виджета нажатием соответствующей иконки:



В разделе «Отображение данных» выбираем «Столбчатая диаграмма».

Включаем использование «Логарифмической шкалы» и «Подписи данных на диаграмме».

Сохраняем получившийся виджет в библиотеку виджетов нажатием соответствующей кнопки.

На вкладке «Система» -> «Отчёты» выбираем созданный ранее отчёт без шаблона и добавляем виджет.

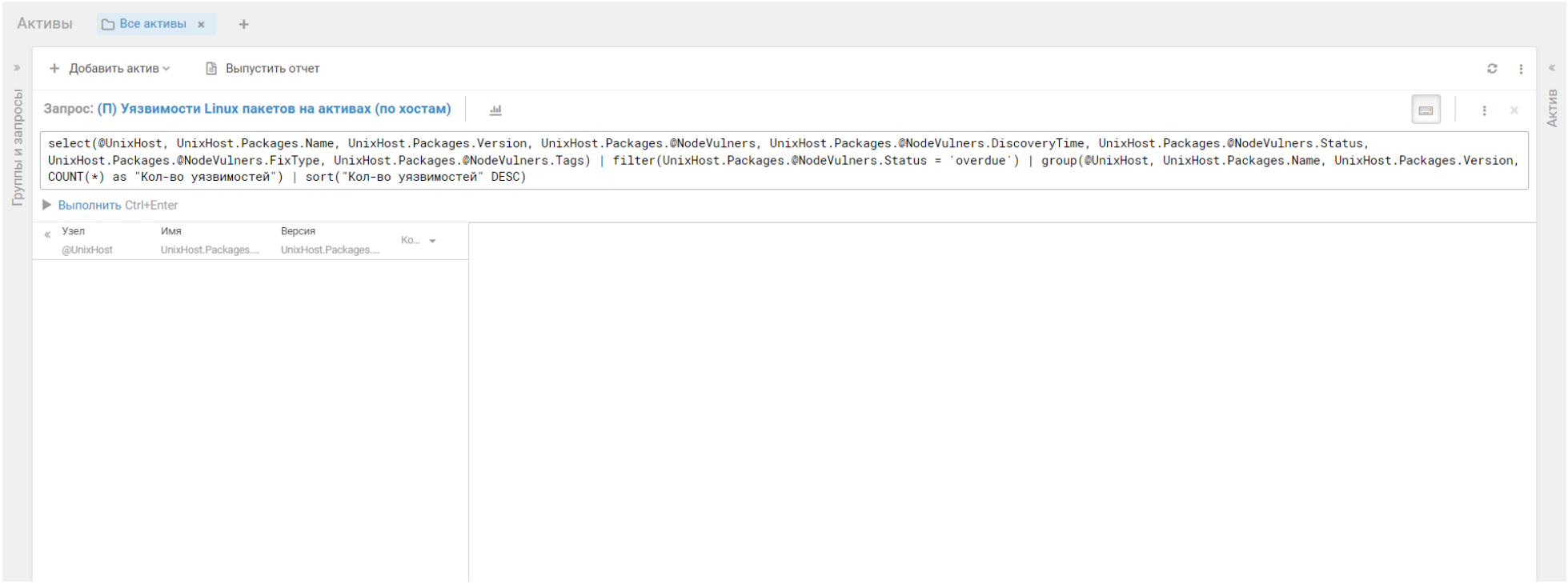
Виджет: «(П) Уязвимости Linux пакетов на активах (по хостам)»

Переходим на вкладку «Активы» и нажимаем на иконку клавиатуры, чтобы перейти к текстовому редактированию запроса.

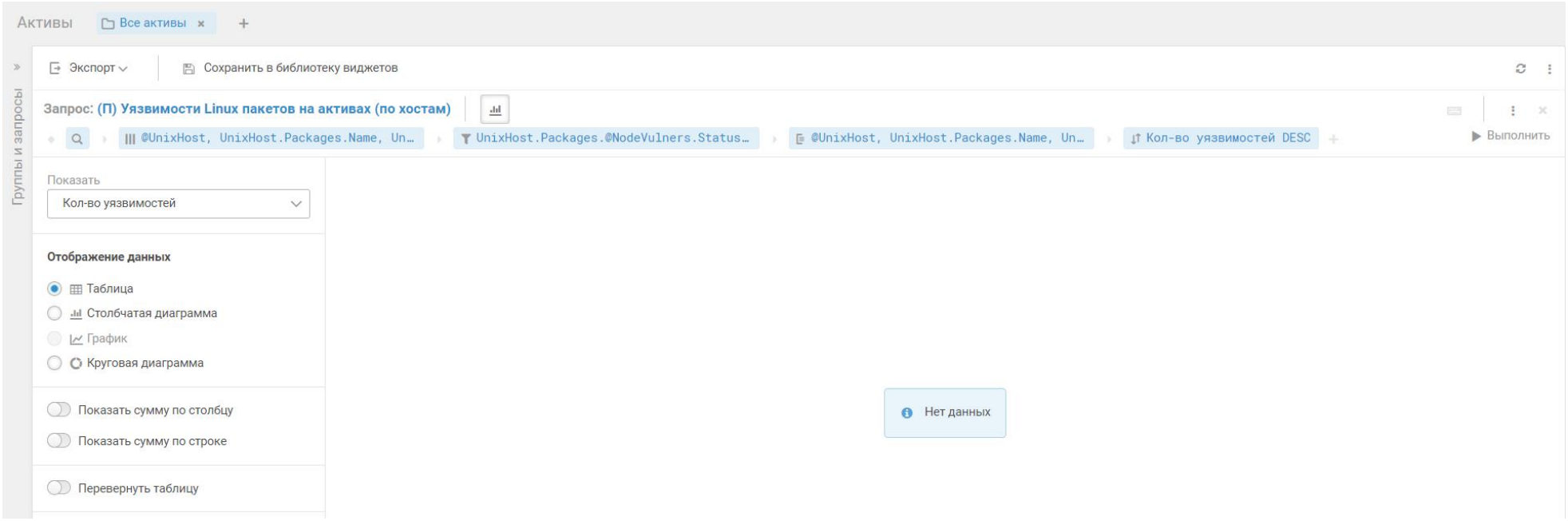
Вставляем и выполняем следующий запрос:

select(@UnixHost, UnixHost.Packages.Name, UnixHost.Packages.Version, UnixHost.Packages.@NodeVulners, UnixHost.Packages.@NodeVulners.DiscoveryTime, UnixHost.Packages.@NodeVulners.Status, UnixHost.Packages.@NodeVulners.FixType, UnixHost.Packages.@NodeVulners.Tags) | filter(UnixHost.Packages.@NodeVulners.Status = 'overdue') | group(@UnixHost, UnixHost.Packages.Name, UnixHost.Packages.Version, COUNT(*) as "Кол-во уязвимостей") | sort("Кол-во уязвимостей" DESC)

*Если в результате выполнения запроса получилась пустая таблица, нарушения регламентов патч-менеджмента IT по данному типу уязвимостей отсутствуют



Переходим в режим создания виджета нажатием соответствующей иконки:



Сохраняем получившийся виджет в библиотеку виджетов нажатием соответствующей кнопки.

На вкладке «Система» -> «Отчёты» выбираем созданный ранее отчёт без шаблона и добавляем виджет.

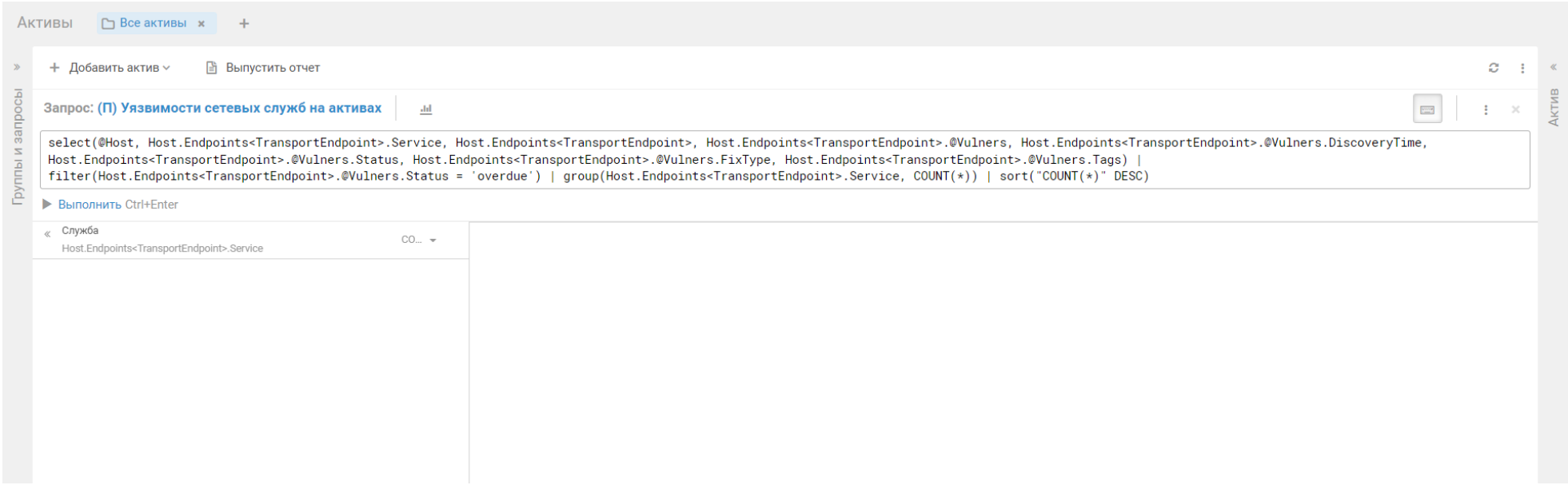
Виджет: «(П) Уязвимости сетевых служб на активах»

Переходим на вкладку «Активы» и нажимаем на иконку клавиатуры, чтобы перейти к текстовому редактированию запроса.

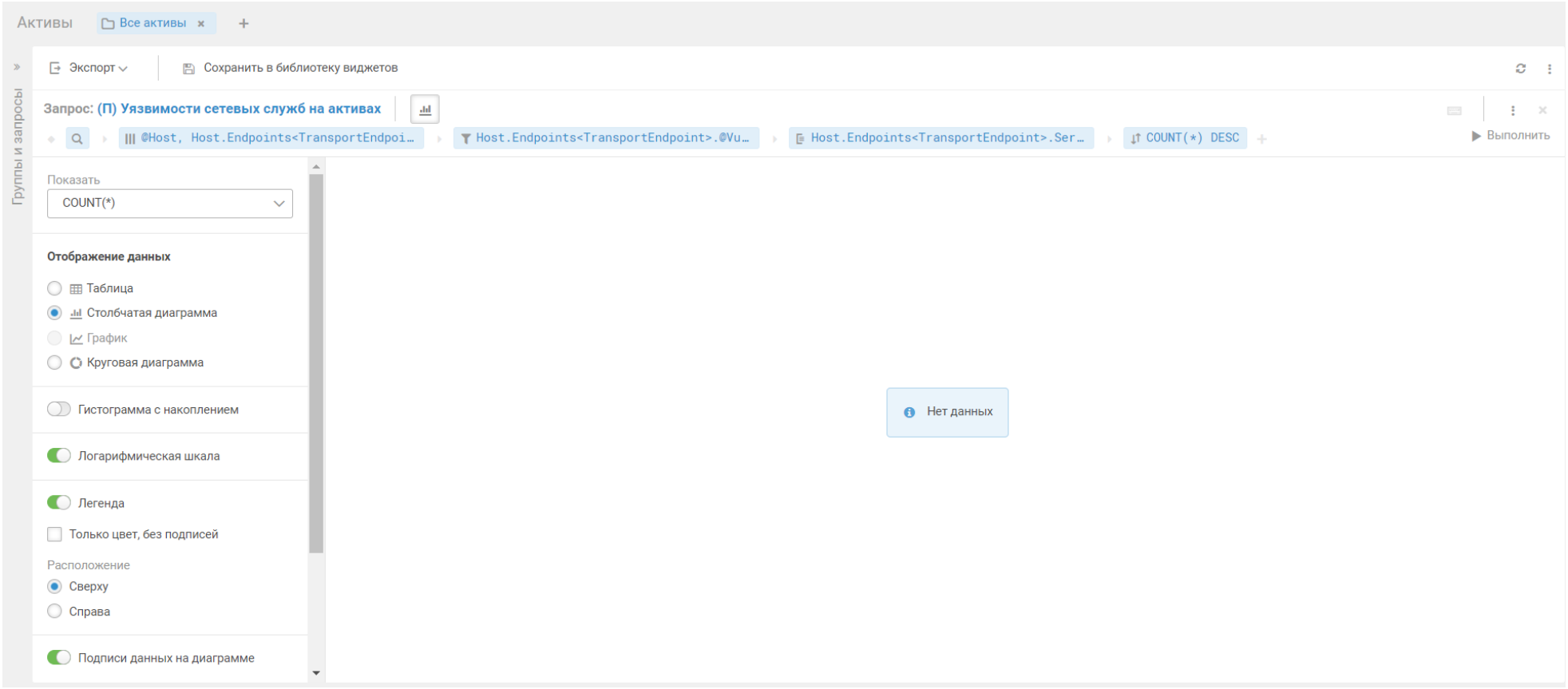
Вставляем и выполняем следующий запрос:

select(@Host, Host.Endpoints<TransportEndpoint>.Service, Host.Endpoints<TransportEndpoint>, Host.Endpoints<TransportEndpoint>.@Vulners, Host.Endpoints<TransportEndpoint>.@Vulners.DiscoveryTime, Host.Endpoints<TransportEndpoint>.@Vulners.Status, Host.Endpoints<TransportEndpoint>.@Vulners.FixType, Host.Endpoints<TransportEndpoint>.@Vulners.Tags) | filter(Host.Endpoints<TransportEndpoint>.@Vulners.Status = 'overdue') | group(Host.Endpoints<TransportEndpoint>.Service, COUNT(*)) | sort("COUNT(*)" DESC)

*Если в результате выполнения запроса получилась пустая таблица, нарушения регламентов патч-менеджмента IT по данному типу уязвимостей отсутствуют



Переходим в режим создания виджета нажатием соответствующей иконки:



В разделе «Отображение данных» выбираем «Столбчатая диаграмма».

Включаем использование «Логарифмической шкалы» и «Подписи данных на диаграмме».

Сохраняем получившийся виджет в библиотеку виджетов нажатием соответствующей кнопки.

На вкладке «Система» -> «Отчёты» выбираем созданный ранее отчёт без шаблона и добавляем виджет.

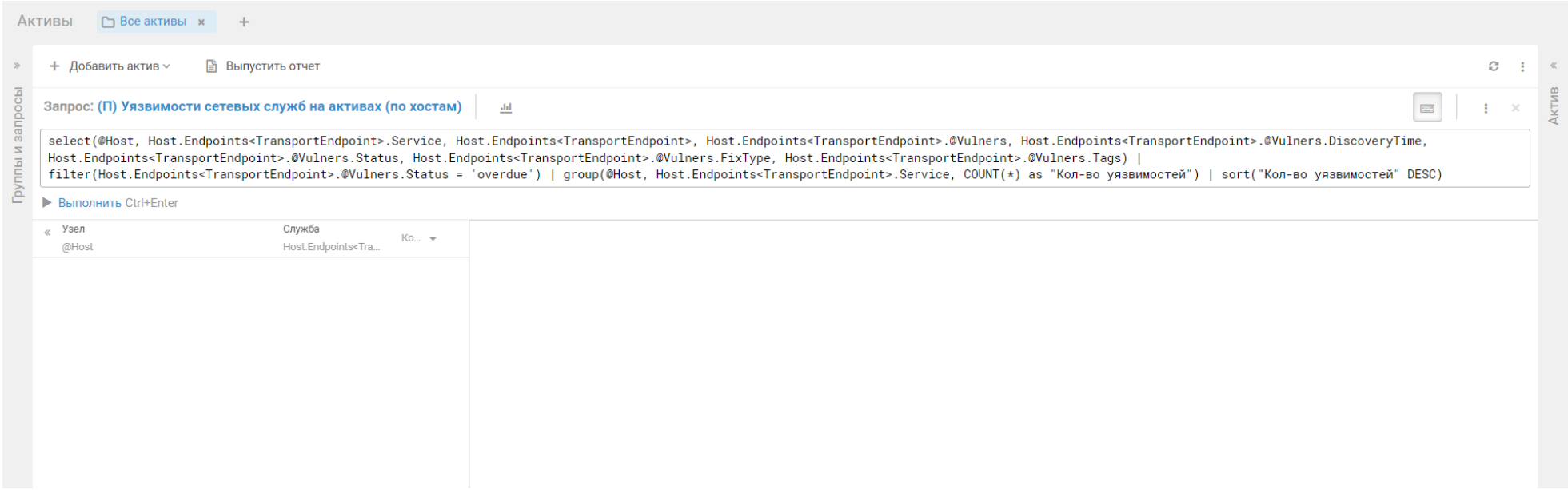
Виджет: «(П) Уязвимости сетевых служб на активах (по хостам)»

Переходим на вкладку «Активы» и нажимаем на иконку клавиатуры, чтобы перейти к текстовому редактированию запроса.

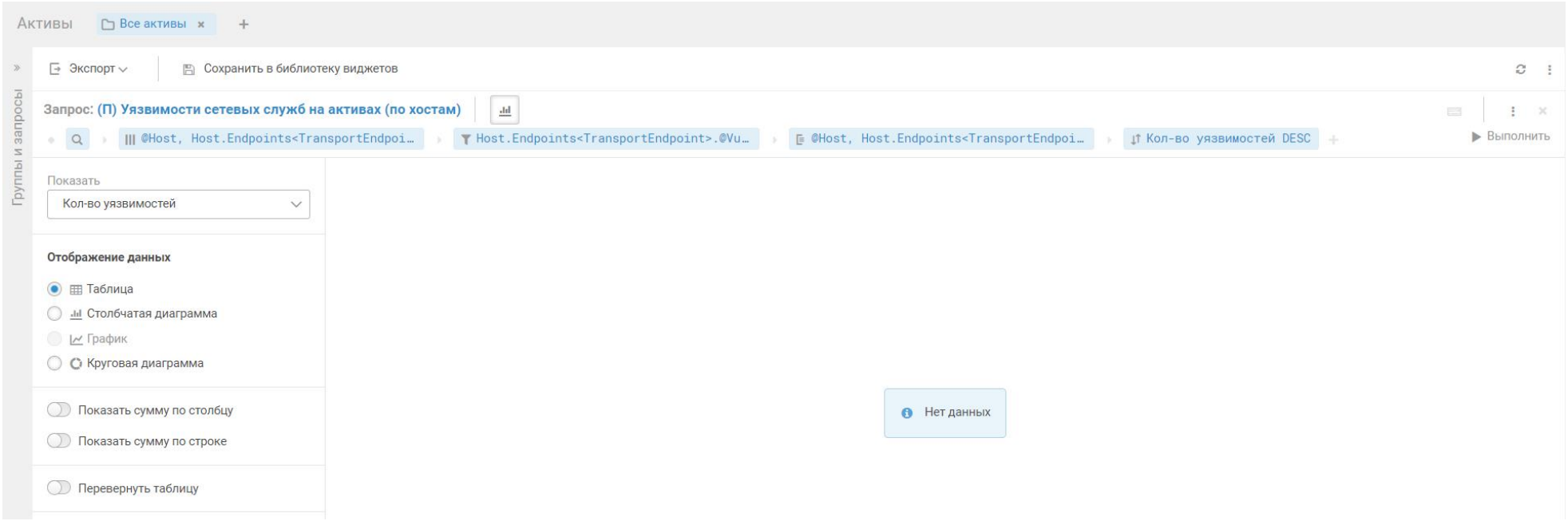
Вставляем и выполняем следующий запрос:

select(@Host, Host.Endpoints<TransportEndpoint>.Service, Host.Endpoints<TransportEndpoint>, Host.Endpoints<TransportEndpoint>.@Vulners, Host.Endpoints<TransportEndpoint>.@Vulners.DiscoveryTime, Host.Endpoints<TransportEndpoint>.@Vulners.Status, Host.Endpoints<TransportEndpoint>.@Vulners.FixType, Host.Endpoints<TransportEndpoint>.@Vulners.Tags) | filter(Host.Endpoints<TransportEndpoint>.@Vulners.Status = 'overdue') | group(@Host, Host.Endpoints<TransportEndpoint>.Service, COUNT(*) as "Кол-во уязвимостей") | sort("Кол-во уязвимостей" DESC)

*Если в результате выполнения запроса получилась пустая таблица, нарушения регламентов патч-менеджмента IT по данному типу уязвимостей отсутствуют



Переходим в режим создания виджета нажатием соответствующей иконки:

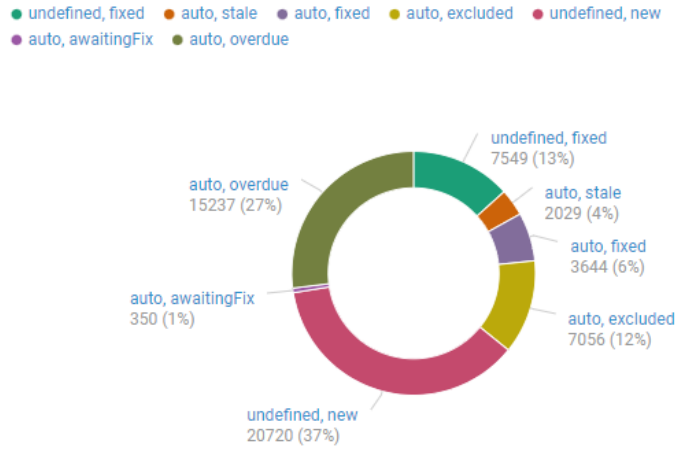


Сохраняем получившийся виджет в библиотеку виджетов нажатием соответствующей кнопки.

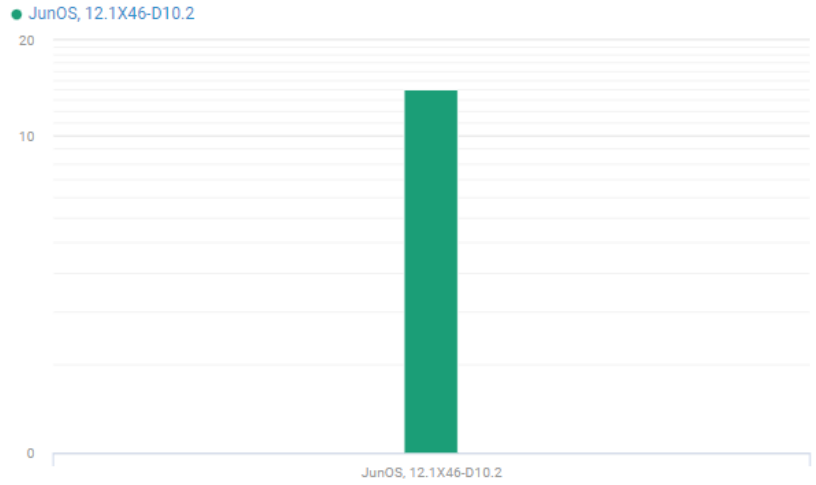
На вкладке «Система» -> «Отчёты» выбираем созданный ранее отчёт без шаблона и добавляем виджет.

7. Отчёт о «слепых зонах» в процессе патч-менеджмента IT

(H) Статистика по статусам покрытия уязвимостей



(H) Уязвимости ОС на активах



(H) Уязвимости ПО на активах

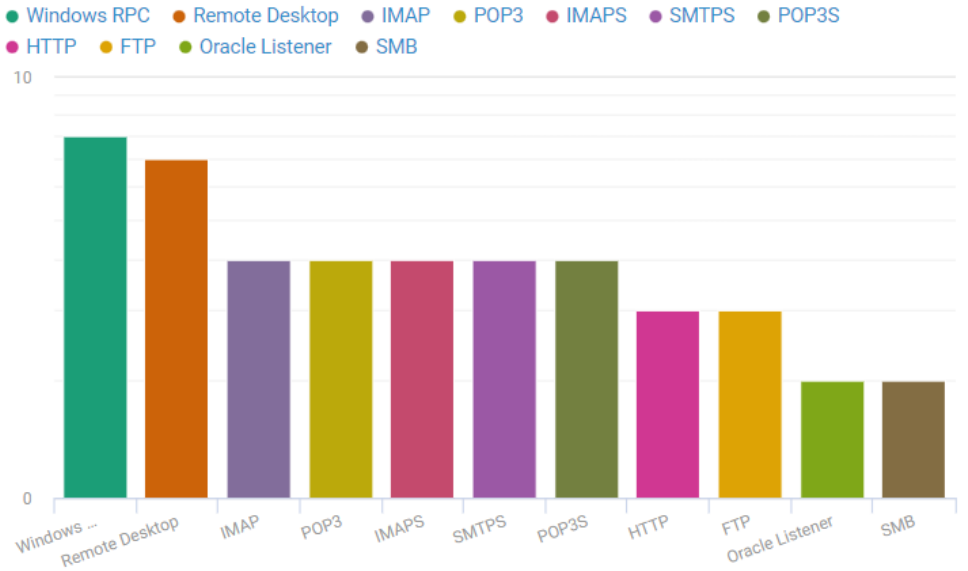
Microsoft Internet Expl... Microsoft Internet Expl... Reader, 11.0.7 iTunes, 12.3.1.23
Microsoft .NET Framew... Microsoft .NET Framew... Java, 8 U77 OpenSSL, 1.0.1p
Microsoft Office, 2013 Google Chrome, 87.0.4... OpenSSL, 1.0.1f
Google Chrome, 88.0.4... OpenSSL, 1.0.1l Google Chrome, 88.0.4...
Microsoft Internet Expl... Microsoft XML Core Se... Google Chrome, 48.0.2...
Microsoft Word, 2013 Opera, 38.0.2220.41 Opera, 39.0.2256.48 FireFox, 41.0.2
Microsoft Office, 2016 Microsoft Office, 2010 Microsoft Excel, 2010
Microsoft .NET Framew... Microsoft Excel, 2016 Microsoft Excel, 2013
Wireshark Network Pro... Java, 8 U281 Microsoft Word, 2010 OpenSSL, 1.0.2m
MySQL Server, 5.1.52 Microsoft Word, 2016 FireFox ESR, 38.3.0
Wireshark Network Pro... Microsoft Outlook, 2013 Microsoft .NET Framew...
Apache HTTP Server, 2... Thunderbird, 38.3.0 OpenSSL, 0.9.8za
Microsoft .NET Framew... OpenSSL, 1.0.1j Microsoft Excel, 2003 OpenSSL, 0.9.8o
OpenSSL, 0.9.8i OpenSSL, 0.9.8t Microsoft Office, 2003 Samba, 3.5.6-86.el6
Microsoft .NET Framew... Microsoft Lync, 2010 Wireshark Network Pro...
Microsoft Word, 2003 Microsoft Outlook, 2016 Microsoft Outlook, 2010
Samba, 3.0.20-Debian OpenSSL, 1.0.2q Bind Server, 9.4.2 Microsoft XML Core Se...
PHP, 5.4.38 Bind Server, 9.10.3-P4 Apache HTTP Server, 2... OpenSSL, 1.0.2j
OpenSSL, 1.0.2r Microsoft PowerPoint, ... Microsoft .NET Framew...
Microsoft Publisher, 20... Silverlight, 5.1.40728.0 Microsoft Internet Expl...
Silverlight, 5.1.20513.0 Microsoft PowerPoint, ... OpenSSL, 0.9.8zc
Microsoft Office Comp... Microsoft Visio, 2003 OpenSSL, 0.9.8zd
Wireshark Network Pro... Foxit Reader, 7.2.2.929 Microsoft .NET Framew...
Microsoft Exchange, 20... VBScript, 5.7.6002.193... PHP, 5.2.4-2ubuntu5.10
Microsoft PowerPoint, ... Microsoft SQL Server, 1... QuickTime Player, 7.78....
Microsoft Remote Desk... Quartzdll, 6.5.2600.5512 Apache Subversion, 1.8...
Microsoft PowerPoint, ... Microsoft Visio, 2013 Microsoft Lync, 2013
OpenSSL, 0.9.8zg 7-Zip, 4.57 Microsoft Visio, 2010 Microsoft Visio Viewer, ...
Microsoft Windows Me... Microsoft SQL Server, 1... Microsoft Access, 2016
JScript, 5.7.6002.19351 Microsoft Publisher, 20... Microsoft Access, 2010
Microsoft Outlook, 2003 Quartzdll, 6.6.7601.175... Microsoft Access, 2013
7-Zip, 18.01 TeamViewer, 10.0.47484 Real Player, 18.1.0.1236
Microsoft Publisher, 20... Microsoft OneNote, 2010 UltraISO, 9.6.5.3237
VBScript, 5.8.7601.175... Microsoft OneNote, 2016 Microsoft Windows Def...
7-Zip, 9.20 Notepad++, 7.5.1 MongoDB, 2.4.9 Microsoft Publisher, 20...
CryptoPro CSP, 3.6.7777 TeamViewer, 15.6.7 Microsoft InfoPath, 2010
Microsoft Access, 2003 OpenVPN, 2.4.6 Microsoft Remote Desk...
Microsoft XML Core Se... Notepad++, 7.7.1 Microsoft Windows Liv...
Microsoft Windows Me... Microsoft OneNote, 2013 Skype, 7.3.101
Microsoft Windows Def... JScript, 5.8.7601.17514 Tor Browser, 5.0.3
JScript, 5.7.0.16599 Skype, 7.13.101

(H) Уязвимости Linux пакетов на активах

- firefox, 0:3.6.17-1.el6_0
- kernel, 0:2.6.32-131.0.1...
- kernel-devel, 0:2.6.32-1...
- kernel-headers, 0:2.6.3...
- iceweasel, 38.8.0esr-1...
- java-1.6.0-openjdk, 1:1....
- vim, 2:7.3.547-7
- vim-runtime, 2:8.1.087...
- vim-tiny, 2:7.4.488-7
- xxd, 2:8.1.0875-5
- vim-tiny, 2:7.3.547-7
- vim-tiny, 2:8.0.0197-4+...
- vim-runtime, 2:7.3.547-7
- vim-runtime, 2:8.0.019...
- vim, 2:8.1.0875-5
- vim, 2:8.0.0197-4+deb9...
- vim-common, 2:8.1.08...
- vim-common, 2:8.0.01...
- xxd, 2:8.0.0197-4+deb9...
- vim-common, 2:7.3.54...
- xorg-x11-server-comm...
- xorg-x11-server-Xorg, 0:...
- libtiff5, 4.0.8-2+deb9u4
- tcpdump, 14:4.0.0-3.20...
- exim4-daemon-light, 4....
- exim4-base, 4.89-2+de...
- exim4-config, 4.89-2+d...
- samba-client, 0:3.5.6-8...
- samba-winbind-clients, ...
- samba, 0:3.5.6-86.el6
- samba-common, 0:3.5....
- libsmbclient, 0:3.5.6-86...
- ntp, 0:4.2.4p8-2.el6
- ntpdate, 0:4.2.4p8-2.el6
- ghostscript, 0:8.70-11.e...
- bind-libs, 32:9.7.3-2.el6
- bind-utils, 32:9.7.3-2.el6
- httpd-tools, 0:2.2.15-26...
- imagemagick-common,...
- libtiff, 0:3.9.4-1.el6_0.3
- httpd, 0:2.2.15-26.el6
- mod_ssl, 1:2.2.15-26.el6
- jasper-libs, 0:1.900.1-1...
- libtiff5, 4.1.0+git19111...
- poppler-glib, 0:0.12.4-3....
- poppler, 0:0.12.4-3.el6_...
- poppler-utils, 0:0.12.4-3...
- nss-tools, 0:3.12.9-9.el6
- nss, 0:3.12.9-9.el6
- nss-sysinit, 0:3.12.9-9.e...
- evince-libs, 0:2.28.2-14....
- evince-dvi, 0:2.28.2-14....
- bind9-host, 1:9.10.3.dfs...
- evince, 0:2.28.2-14.el6_...
- libgs9-common, 9.05~...
- libgs9, 9.05~dfsg-6.3+...
- gdm, 1:2.30.4-21.el6_0.1
- ipa-client, 0:2.0.0-23.el6
- nss-util, 0:3.12.9-1.el6
- libarchive, 0:2.8.3-2.el6
- freetype, 0:2.3.11-6.el6...
- xulrunner, 0:1.9.2.17-4....
- python-devel, 0:2.6.6-2...
- python, 0:2.6.6-20.el6
- python-libs, 0:2.6.6-20....
- libcurl3-gnutls, 7.52.1-5...
- curl, 7.52.1-5+deb9u10
- libcurl3-gnutls, 7.52.1-5...
- curl, 7.38.0-4+deb8u9
- libcurl3-gnutls, 7.26.0-1...
- postgresql-server, 0:8.4...
- postgresql, 0:8.4.7-2.el6
- postgresql-contrib, 0:8....
- xserver-common, 2:1.1...
- tcpdump, 4.9.3-1~deb9...
- xserver-xorg-core, 2:1.1...
- postgresql-libs, 0:8.4.7-...
- krb5-devel, 0:1.9-9.el6
- krb5-workstation, 0:1.9-...
- binutils, 0:2.20.51.0.2-5...
- krb5-libs, 0:1.9-9.el6
- autocorr-en, 1:3.2.1-19....
- exim4-base, 4.80-7+de...
- exim4-config, 4.80-7+d...
- exim4, 4.89-2+deb9u6
- exim4, 4.80-7+deb7u3
- exim4-daemon-light, 4....
- gstreamer-plugins-goo...
- curl, 0:7.19.7-26.el6
- libcurl, 0:7.19.7-26.el6
- nss-softokn, 0:3.12.9-3....
- nss-softokn-freebl, 0:3....
- libexpat1, 2.2.0-2+deb9...
- libexpat1, 2.1.0-1+deb7...
- libssl1.1, 1.1.0l-1~deb9...
- libX11, 0:1.3-2.el6
- openssl, 1.1.0l-1~deb9...

(H) Уязвимости сетевых служб на активах

Источник	Активы
Период обновления	на текущий момент
Группы активов	Все группы
Фильтр	(H) Уязвимости сетевых служб на активах

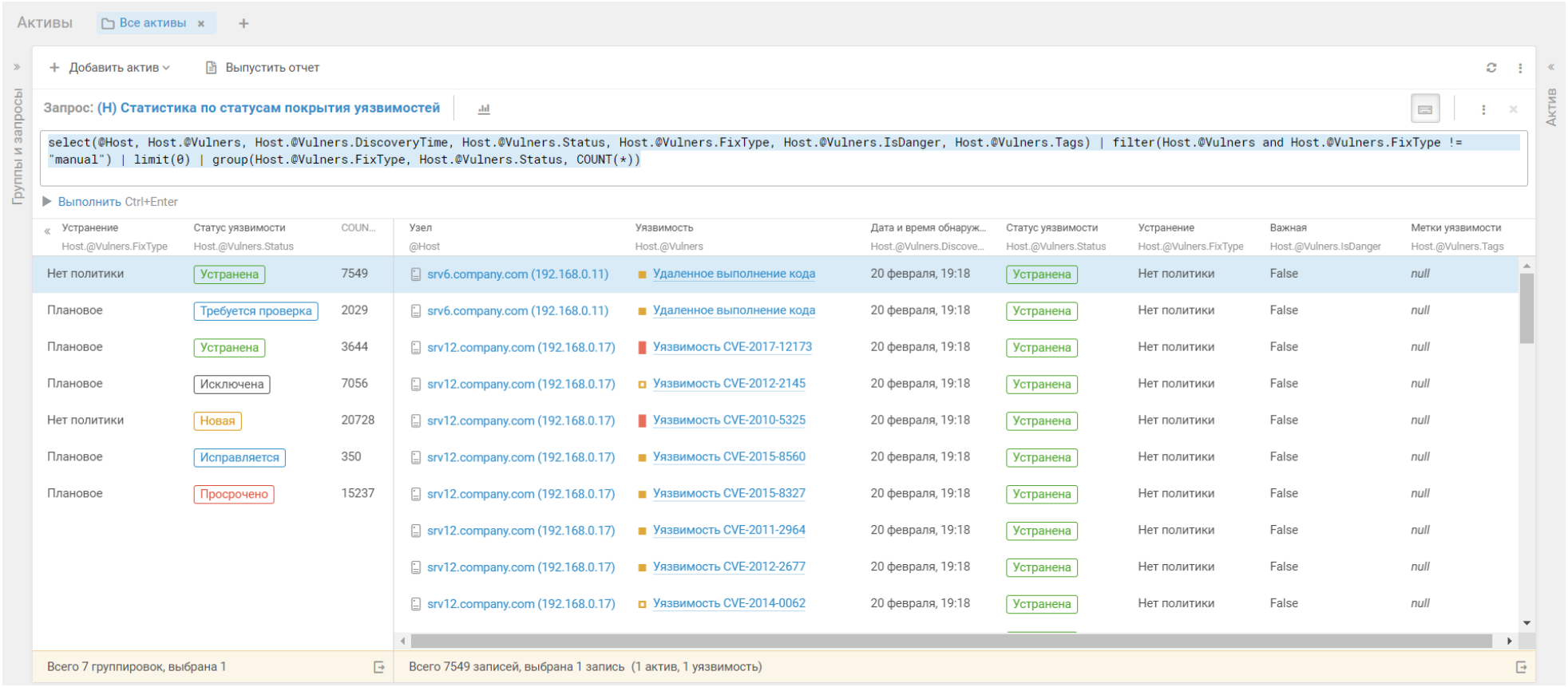


Виджет: «(H) Статистика по статусам покрытия уязвимостей»

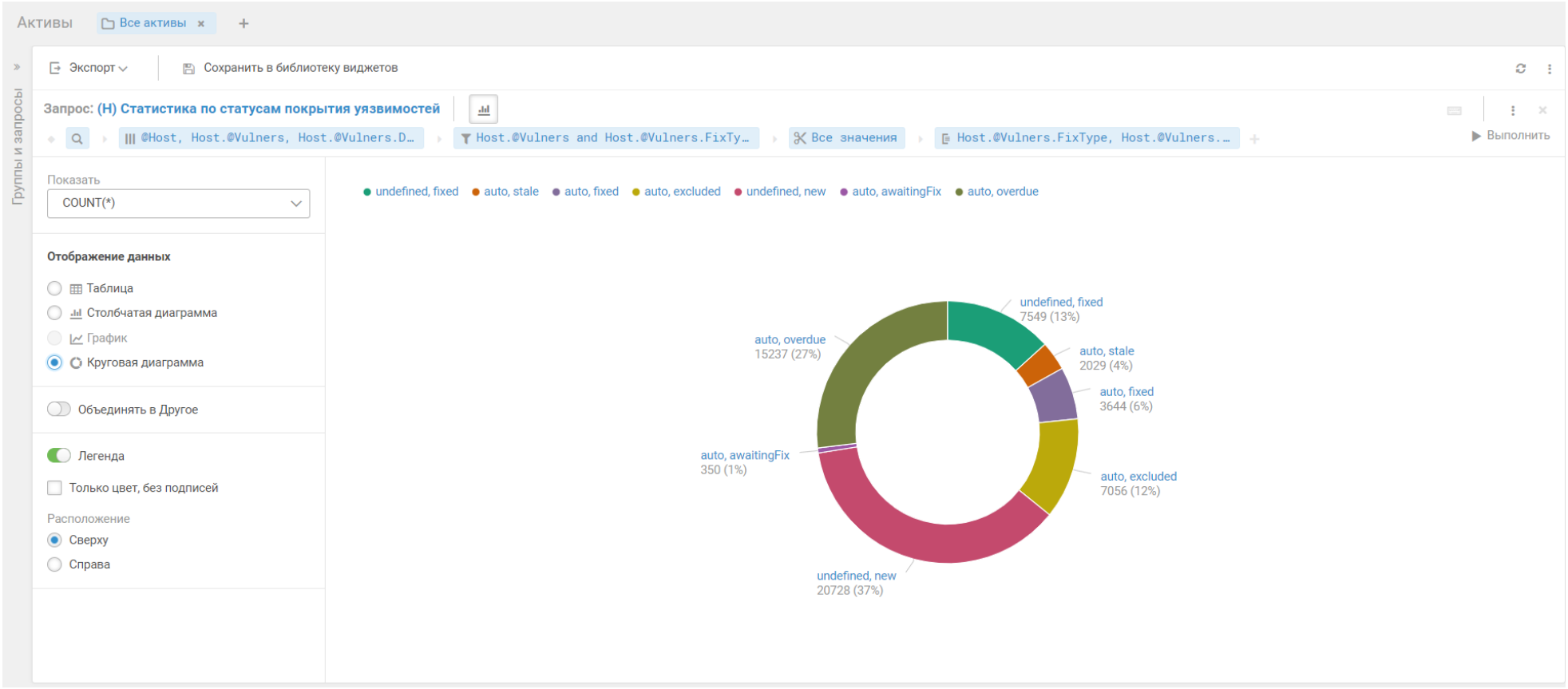
Переходим на вкладку «Активы» и нажимаем на иконку клавиатуры, чтобы перейти к текстовому редактированию запроса.

Вставляем и выполняем следующий запрос:

select(@Host, Host.@Vulners, Host.@Vulners.DiscoveryTime, Host.@Vulners.Status, Host.@Vulners.FixType, Host.@Vulners.IsDanger, Host.@Vulners.Tags) | filter(Host.@Vulners and Host.@Vulners.FixType != "manual") | limit(0) | group(Host.@Vulners.FixType, Host.@Vulners.Status, COUNT(*))



Переходим в режим создания виджета нажатием соответствующей иконки:



В разделе «Отображение данных» выбираем «Круговая диаграмма».

Сохраняем получившийся виджет в библиотеку виджетов нажатием соответствующей кнопки.

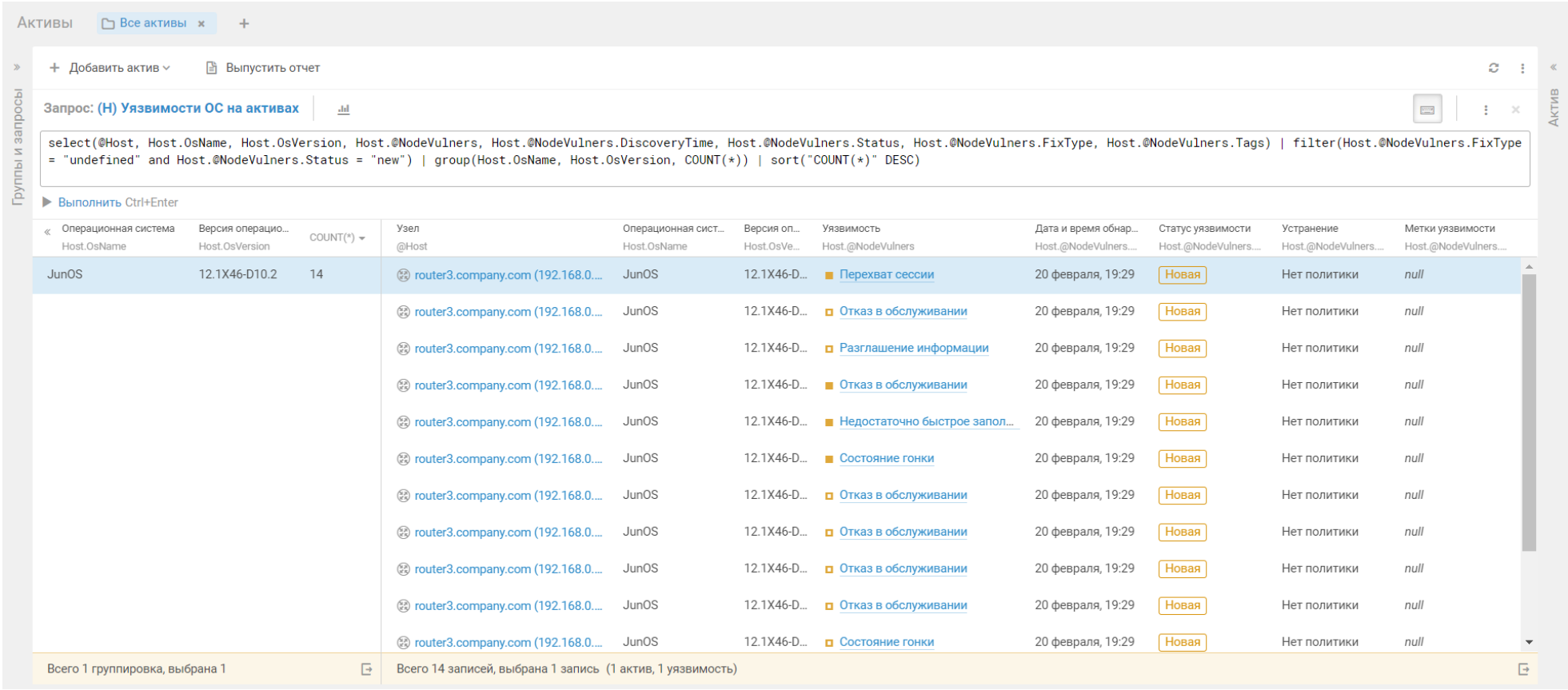
На вкладке «Система» -> «Отчёты» создаём новый отчёт без шаблона и добавляем созданный ранее виджет.

Виджет: «(H) Уязвимости ОС на активах»

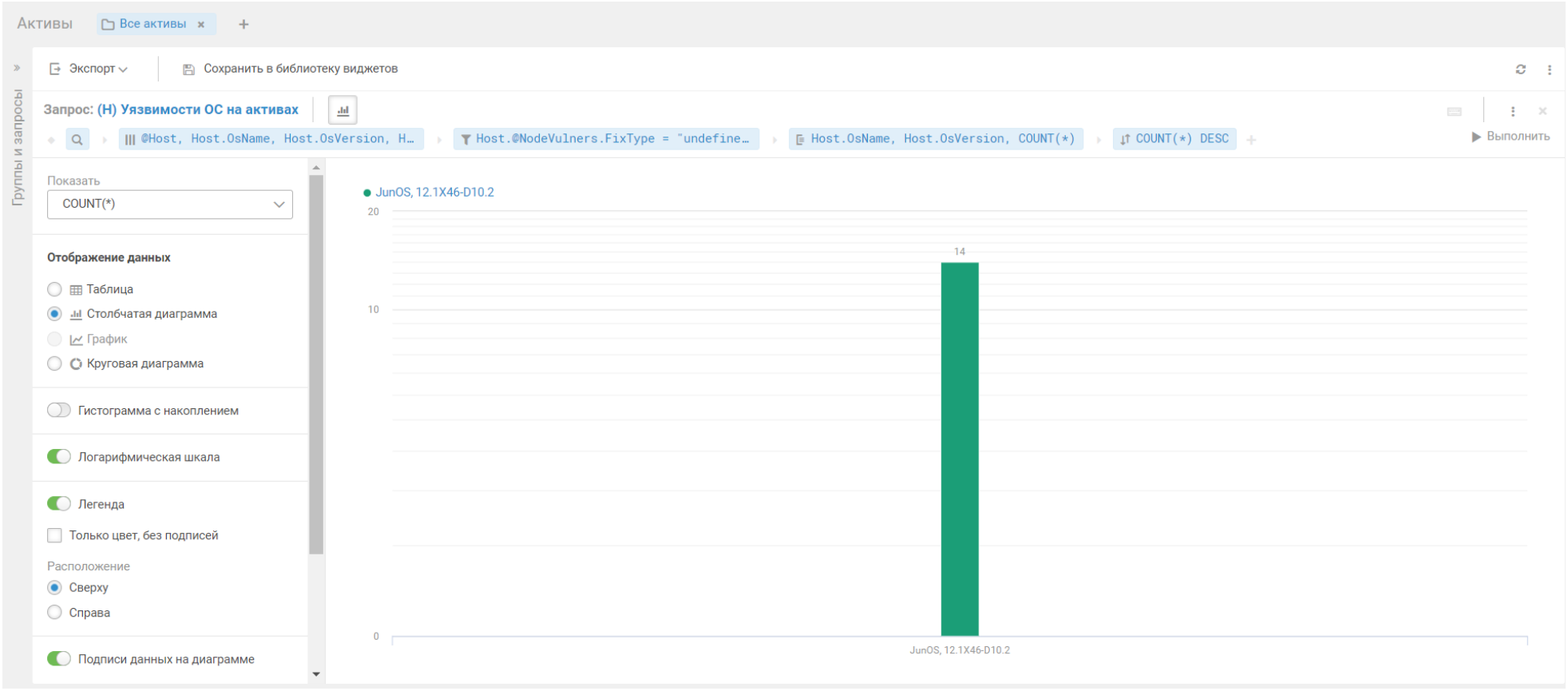
Переходим на вкладку «Активы» и нажимаем на иконку клавиатуры, чтобы перейти к текстовому редактированию запроса.

Вставляем и выполняем следующий запрос:

select(@Host, Host.OsName, Host.OsVersion, Host.@NodeVulners, Host.@NodeVulners.DiscoveryTime, Host.@NodeVulners.Status, Host.@NodeVulners.FixType, Host.@NodeVulners.Tags) | filter(Host.@NodeVulners.FixType = "undefined" and Host.@NodeVulners.Status = "new") | group(Host.OsName, Host.OsVersion, COUNT(*)) | sort("COUNT(*)" DESC)



Переходим в режим создания виджета нажатием соответствующей иконки:



В разделе «Отображение данных» выбираем «Столбчатая диаграмма».

Включаем использование «Логарифмической шкалы» и «Подписи данных на диаграмме».

Сохраняем получившийся виджет в библиотеку виджетов нажатием соответствующей кнопки.

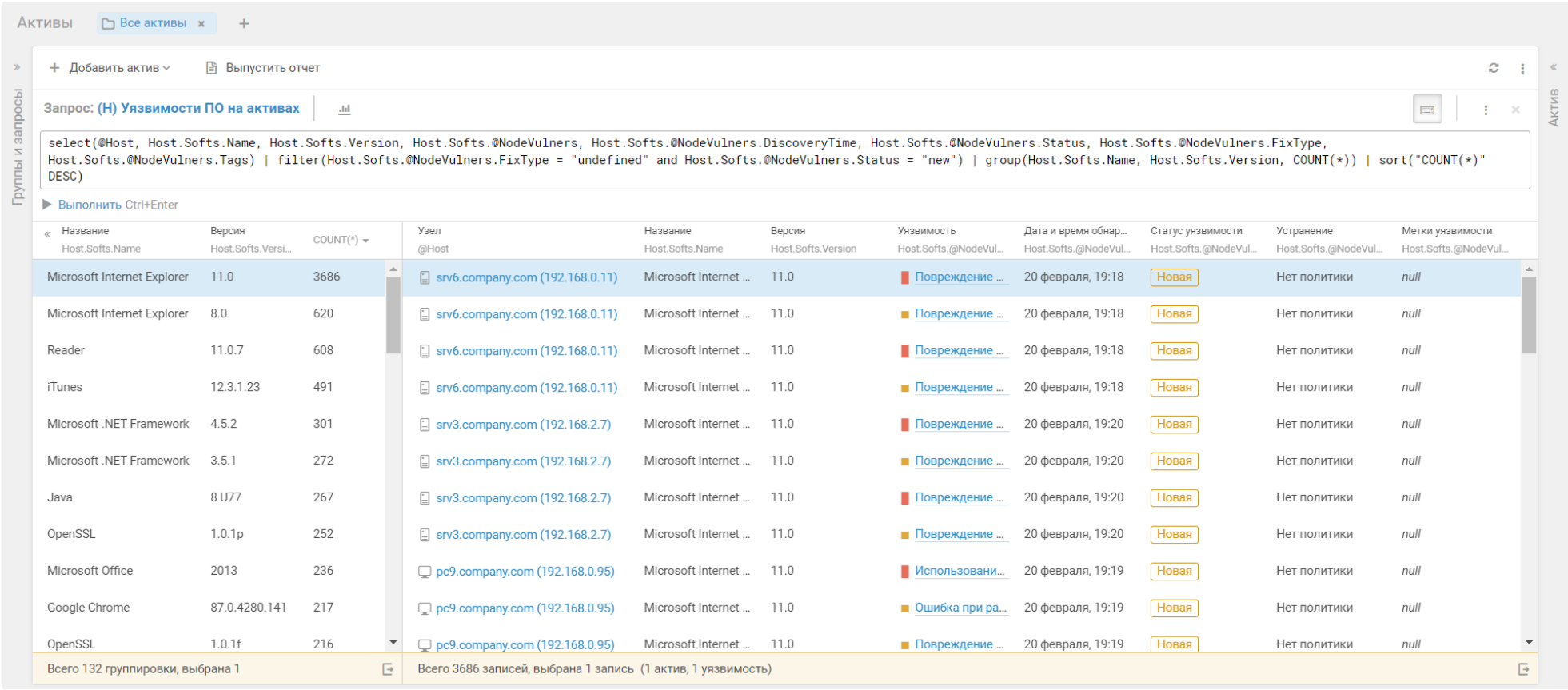
На вкладке «Система» -> «Отчёты» выбираем созданный ранее отчёт без шаблона и добавляем виджет.

Виджет: «(Н) Уязвимости ПО на активах»

Переходим на вкладку «Активы» и нажимаем на иконку клавиатуры, чтобы перейти к текстовому редактированию запроса.

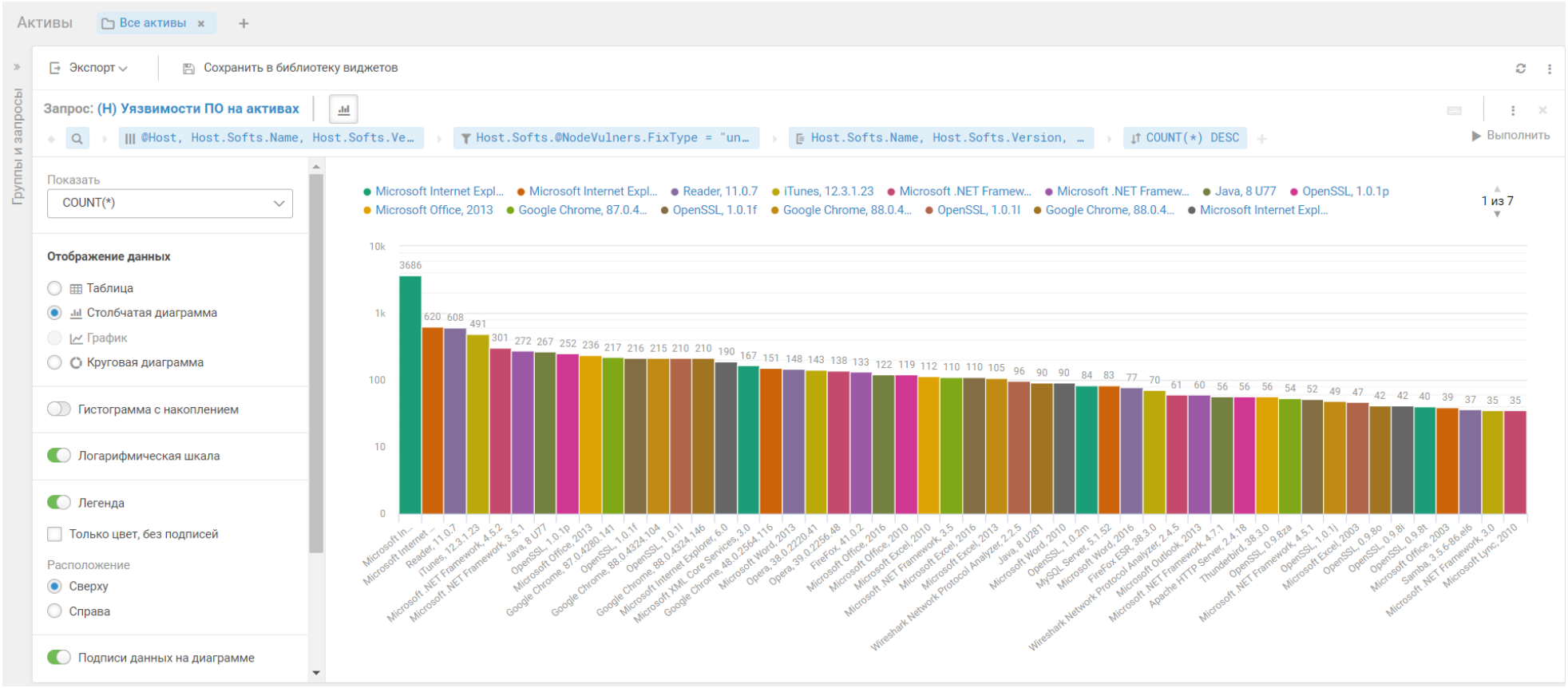
Вставляем и выполняем следующий запрос:

select(@Host, Host.Softs.Name, Host.Softs.Version, Host.Softs.@NodeVulners, Host.Softs.@NodeVulners.DiscoveryTime, Host.Softs.@NodeVulners.Status, Host.Softs.@NodeVulners.FixType, Host.Softs.@NodeVulners.Tags) | filter(Host.Softs.@NodeVulners.FixType = "undefined" and Host.Softs.@NodeVulners.Status = "new") | group(Host.Softs.Name, Host.Softs.Version, COUNT(*)) | sort("COUNT(*)" DESC)



Название Host.Softs.Name	Версия Host.Softs.Versi...	COUNT(*)	Узел @Host	Название Host.Softs.Name	Версия Host.Softs.Version	Уязвимость Host.Softs.@NodeVul...	Дата и время обнар... Host.Softs.@NodeVul...	Статус уязвимости Host.Softs.@NodeVul...	Устранение Host.Softs.@NodeVul...	Метки уязвимости Host.Softs.@NodeVul...
Microsoft Internet Explorer	11.0	3686	srv6.company.com (192.168.0.11)	Microsoft Internet ...	11.0	Повреждение ...	20 февраля, 19:18	Новая	Нет политики	null
Microsoft Internet Explorer	8.0	620	srv6.company.com (192.168.0.11)	Microsoft Internet ...	11.0	Повреждение ...	20 февраля, 19:18	Новая	Нет политики	null
Reader	11.0.7	608	srv6.company.com (192.168.0.11)	Microsoft Internet ...	11.0	Повреждение ...	20 февраля, 19:18	Новая	Нет политики	null
iTunes	12.3.1.23	491	srv6.company.com (192.168.0.11)	Microsoft Internet ...	11.0	Повреждение ...	20 февраля, 19:18	Новая	Нет политики	null
Microsoft .NET Framework	4.5.2	301	srv3.company.com (192.168.2.7)	Microsoft Internet ...	11.0	Повреждение ...	20 февраля, 19:20	Новая	Нет политики	null
Microsoft .NET Framework	3.5.1	272	srv3.company.com (192.168.2.7)	Microsoft Internet ...	11.0	Повреждение ...	20 февраля, 19:20	Новая	Нет политики	null
Java	8 U77	267	srv3.company.com (192.168.2.7)	Microsoft Internet ...	11.0	Повреждение ...	20 февраля, 19:20	Новая	Нет политики	null
OpenSSL	1.0.1p	252	srv3.company.com (192.168.2.7)	Microsoft Internet ...	11.0	Повреждение ...	20 февраля, 19:20	Новая	Нет политики	null
Microsoft Office	2013	236	pc9.company.com (192.168.0.95)	Microsoft Internet ...	11.0	Использовани...	20 февраля, 19:19	Новая	Нет политики	null
Google Chrome	87.0.4280.141	217	pc9.company.com (192.168.0.95)	Microsoft Internet ...	11.0	Ошибка при ра...	20 февраля, 19:19	Новая	Нет политики	null
OpenSSL	1.0.1f	216	pc9.company.com (192.168.0.95)	Microsoft Internet ...	11.0	Повреждение ...	20 февраля, 19:19	Новая	Нет политики	null

Переходим в режим создания виджета нажатием соответствующей иконки:



В разделе «Отображение данных» выбираем «Столбчатая диаграмма».

Включаем использование «Логарифмической шкалы» и «Подписи данных на диаграмме».

Сохраняем получившийся виджет в библиотеку виджетов нажатием соответствующей кнопки.

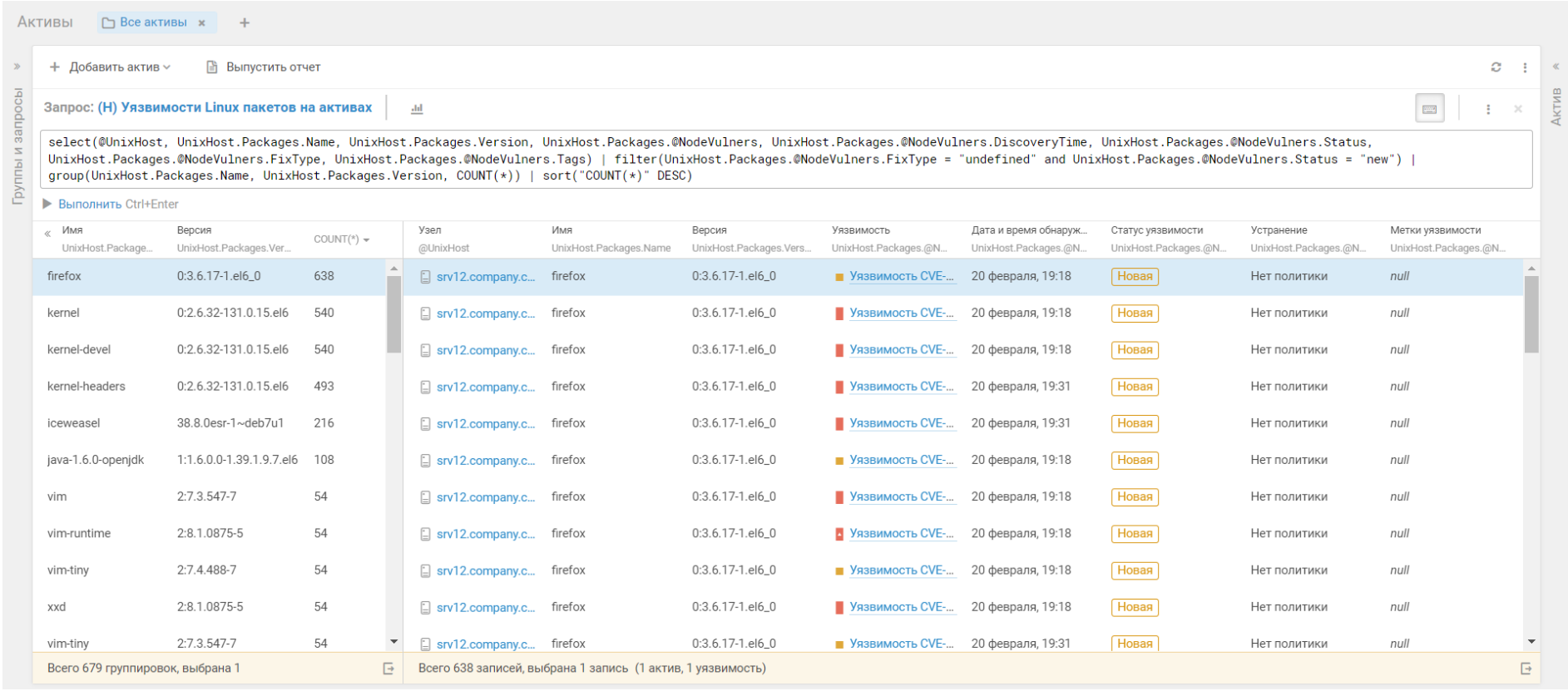
На вкладке «Система» -> «Отчёты» выбираем созданный ранее отчёт без шаблона и добавляем виджет.

Виджет: «(H) Уязвимости Linux пакетов на активах»

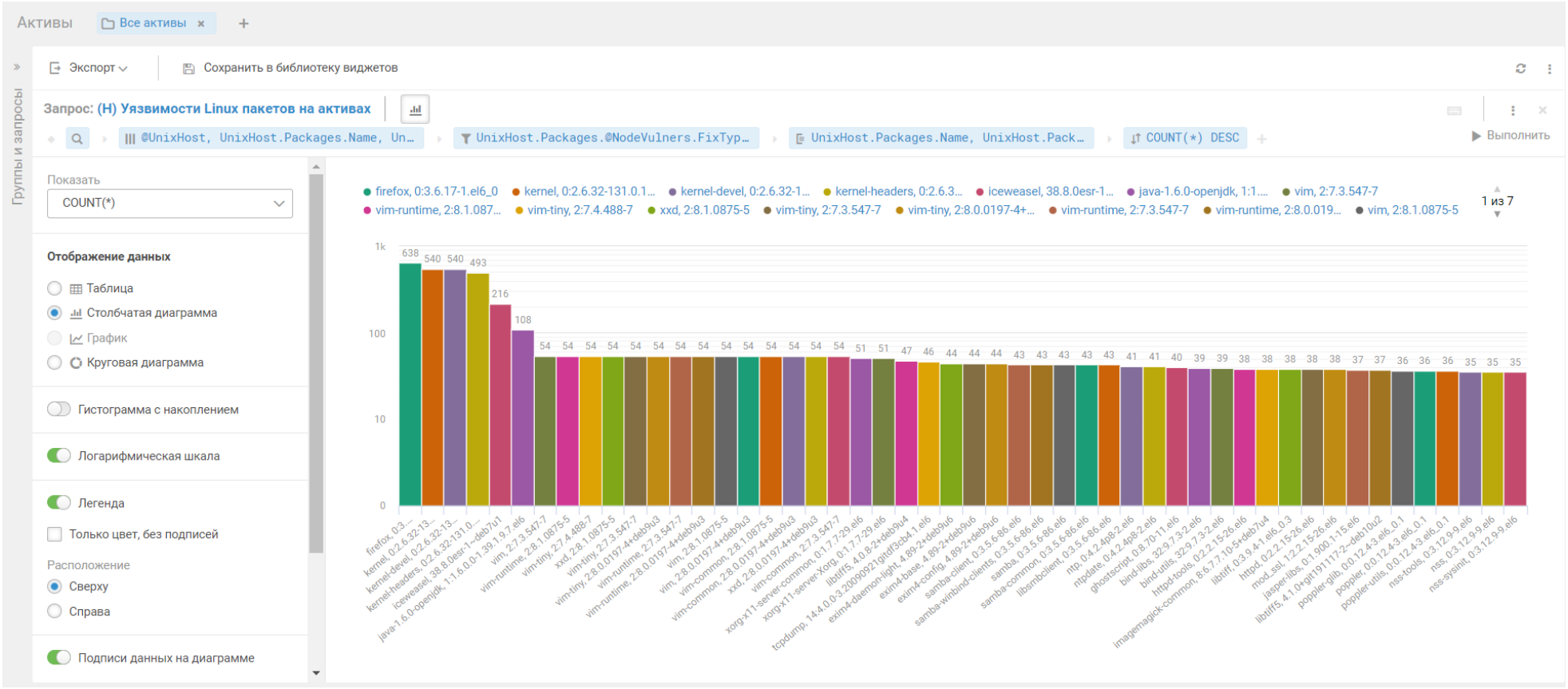
Переходим на вкладку «Активы» и нажимаем на иконку клавиатуры, чтобы перейти к текстовому редактированию запроса.

Вставляем и выполняем следующий запрос:

select(@UnixHost, UnixHost.Packages.Name, UnixHost.Packages.Version, UnixHost.Packages.@NodeVulners, UnixHost.Packages.@NodeVulners.DiscoveryTime, UnixHost.Packages.@NodeVulners.Status, UnixHost.Packages.@NodeVulners.FixType, UnixHost.Packages.@NodeVulners.Tags) | filter(UnixHost.Packages.@NodeVulners.FixType = "undefined" and UnixHost.Packages.@NodeVulners.Status = "new") | group(UnixHost.Packages.Name, UnixHost.Packages.Version, COUNT(*)) | sort("COUNT(*)" DESC)



Переходим в режим создания виджета нажатием соответствующей иконки:



В разделе «Отображение данных» выбираем «Столбчатая диаграмма».

Включаем использование «Логарифмической шкалы» и «Подписи данных на диаграмме».

Сохраняем получившийся виджет в библиотеку виджетов нажатием соответствующей кнопки.

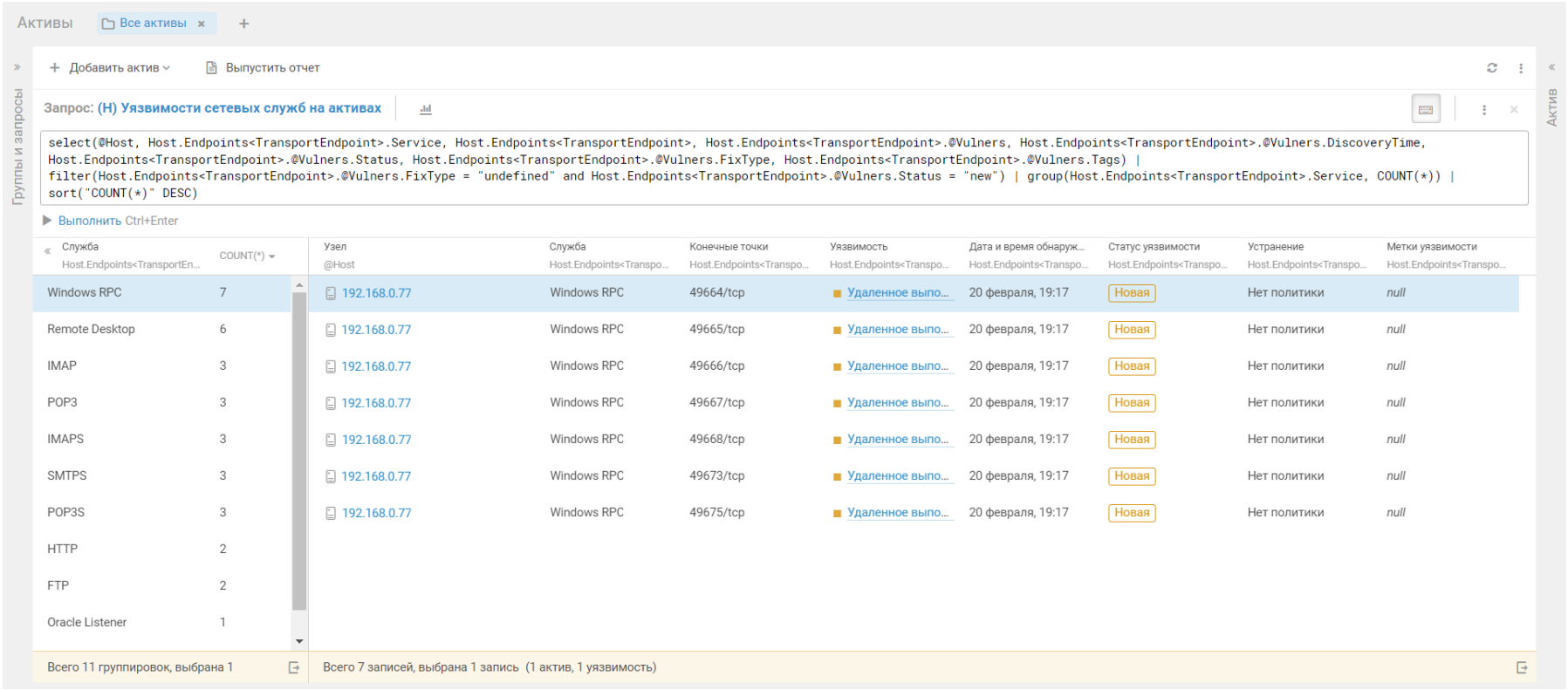
На вкладке «Система» -> «Отчёты» выбираем созданный ранее отчёт без шаблона и добавляем виджет.

Виджет: «(H) Уязвимости сетевых служб на активах»

Переходим на вкладку «Активы» и нажимаем на иконку клавиатуры, чтобы перейти к текстовому редактированию запроса.

Вставляем и выполняем следующий запрос:

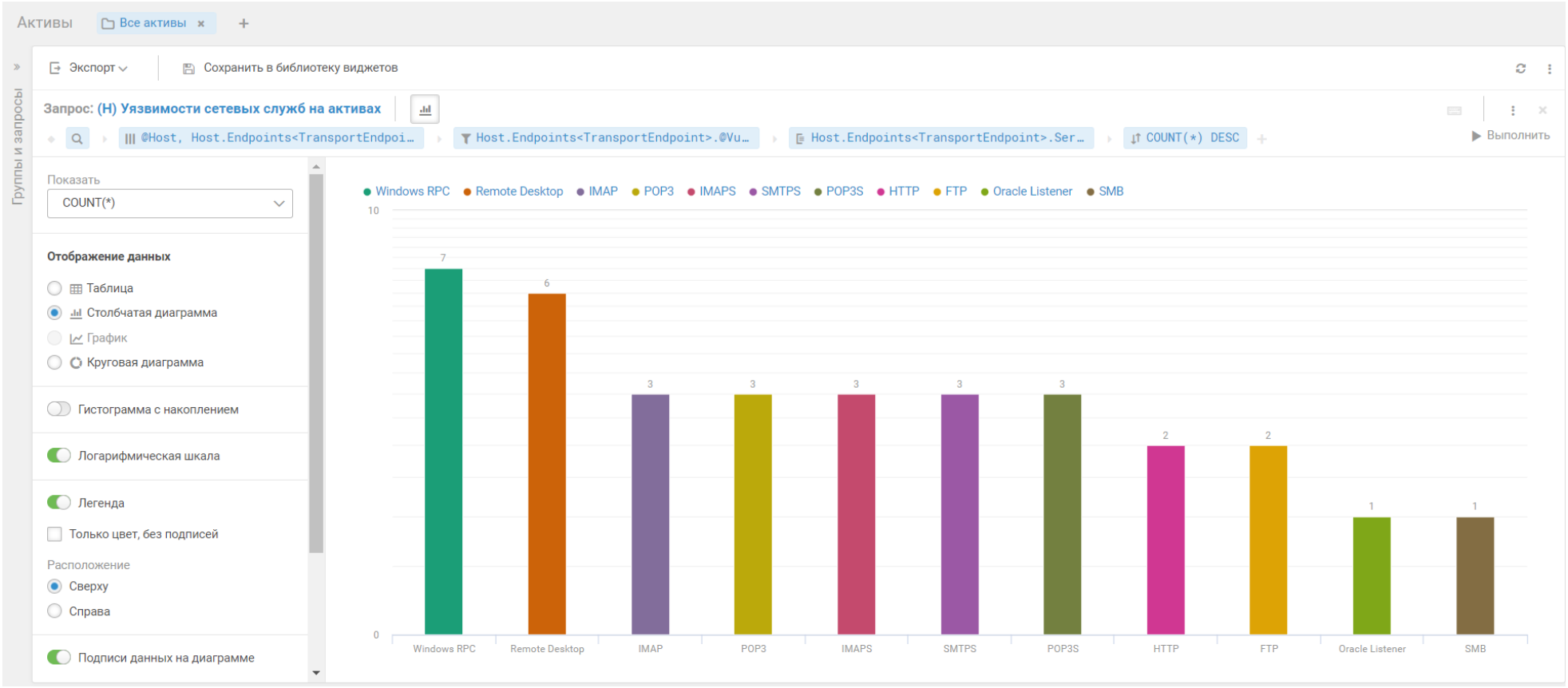
select(@Host, Host.Endpoints<TransportEndpoint>.Service, Host.Endpoints<TransportEndpoint>, Host.Endpoints<TransportEndpoint>.@Vulners, Host.Endpoints<TransportEndpoint>.@Vulners.DiscoveryTime, Host.Endpoints<TransportEndpoint>.@Vulners.Status, Host.Endpoints<TransportEndpoint>.@Vulners.FixType, Host.Endpoints<TransportEndpoint>.@Vulners.Tags) | filter(Host.Endpoints<TransportEndpoint>.@Vulners.FixType = "undefined" and Host.Endpoints<TransportEndpoint>.@Vulners.Status = "new") | group(Host.Endpoints<TransportEndpoint>.Service, COUNT(*)) | sort("COUNT(*)" DESC)



Служба	COUNT(*)
Windows RPC	7
Remote Desktop	6
IMAP	3
POP3	3
IMAPS	3
SMTPS	3
POP3S	3
HTTP	2
FTP	2
Oracle Listener	1

Узел	Служба	Конечные точки	Уязвимость	Дата и время обнаруж...	Статус уязвимости	Устранение	Метки уязвимости
192.168.0.77	Windows RPC	49664/tcp	Удаленное выпо...	20 февраля, 19:17	Новая	Нет политики	null
192.168.0.77	Windows RPC	49665/tcp	Удаленное выпо...	20 февраля, 19:17	Новая	Нет политики	null
192.168.0.77	Windows RPC	49666/tcp	Удаленное выпо...	20 февраля, 19:17	Новая	Нет политики	null
192.168.0.77	Windows RPC	49667/tcp	Удаленное выпо...	20 февраля, 19:17	Новая	Нет политики	null
192.168.0.77	Windows RPC	49668/tcp	Удаленное выпо...	20 февраля, 19:17	Новая	Нет политики	null
192.168.0.77	Windows RPC	49673/tcp	Удаленное выпо...	20 февраля, 19:17	Новая	Нет политики	null
192.168.0.77	Windows RPC	49675/tcp	Удаленное выпо...	20 февраля, 19:17	Новая	Нет политики	null

Переходим в режим создания виджета нажатием соответствующей иконки:



В разделе «Отображение данных» выбираем «Столбчатая диаграмма».

Включаем использование «Логарифмической шкалы» и «Подписи данных на диаграмме».

Сохраняем получившийся виджет в библиотеку виджетов нажатием соответствующей кнопки.

На вкладке «Система» -> «Отчёты» выбираем созданный ранее отчёт без шаблона и добавляем виджет.

8. Устранение трендовых уязвимостей

Патчинг уязвимости: CVE-2022-22242

Уязвимость	Количество		
XSS уязвимость в веб-интерфейсе J-Web операционной системы JunOS CVE-2022-22242 juniper Juniper JUNOS	1	0	0

XSS уязвимость в веб-интерфейсе J-Web операционной системы JunOS

CVE-2022-22242 juniper Juniper JUNOS

Трендовая | Удаленно | 1 | 0 | 0

Эксплуатация этой уязвимости может привести к использованию существующей сессии администратора удалённым атакующим. Также она может использоваться в связке с другими уязвимостями, требующими наличие авторизации

Дата публикации
12 октября 2022, 03:00

Как исправить
Производитель выпустил версии софта, исправляющие данную уязвимость. Исправленные версии:
Junos OS 19.1R3-S9, 19.2R3-S6, 19.3R3-S7, 19.4R3-S9, 20.1R3-S5, 20.2R3-S5, 20.3R3-S5, 20.4R3-S4, 21.1R3-S2, 21.3R3, 21.4R3, 22.1R2, 22.2R1, и все последующие.

При невозможности установить обновление, производитель рекомендует отключить веб-интерфейс, либо ограничить доступ к нему только с доверенных источников.

Статус	Уязвимость на активе	Обнаружена
Новая	router3.company.com (192.168.0.245) Важная Устранение: Вручную juniper Juniper JUNOS 12.1X46-D10.2	20 фев, 19:29

На вкладке «Система» -> «Отчёты» создаём новый отчёт без шаблона.

Виджет: «Патчинг уязвимости: CVE-2022-22242»

Добавляем стандартный виджет «Список уязвимостей».

В настройках виджета указываем:

На вкладке «Отображение»

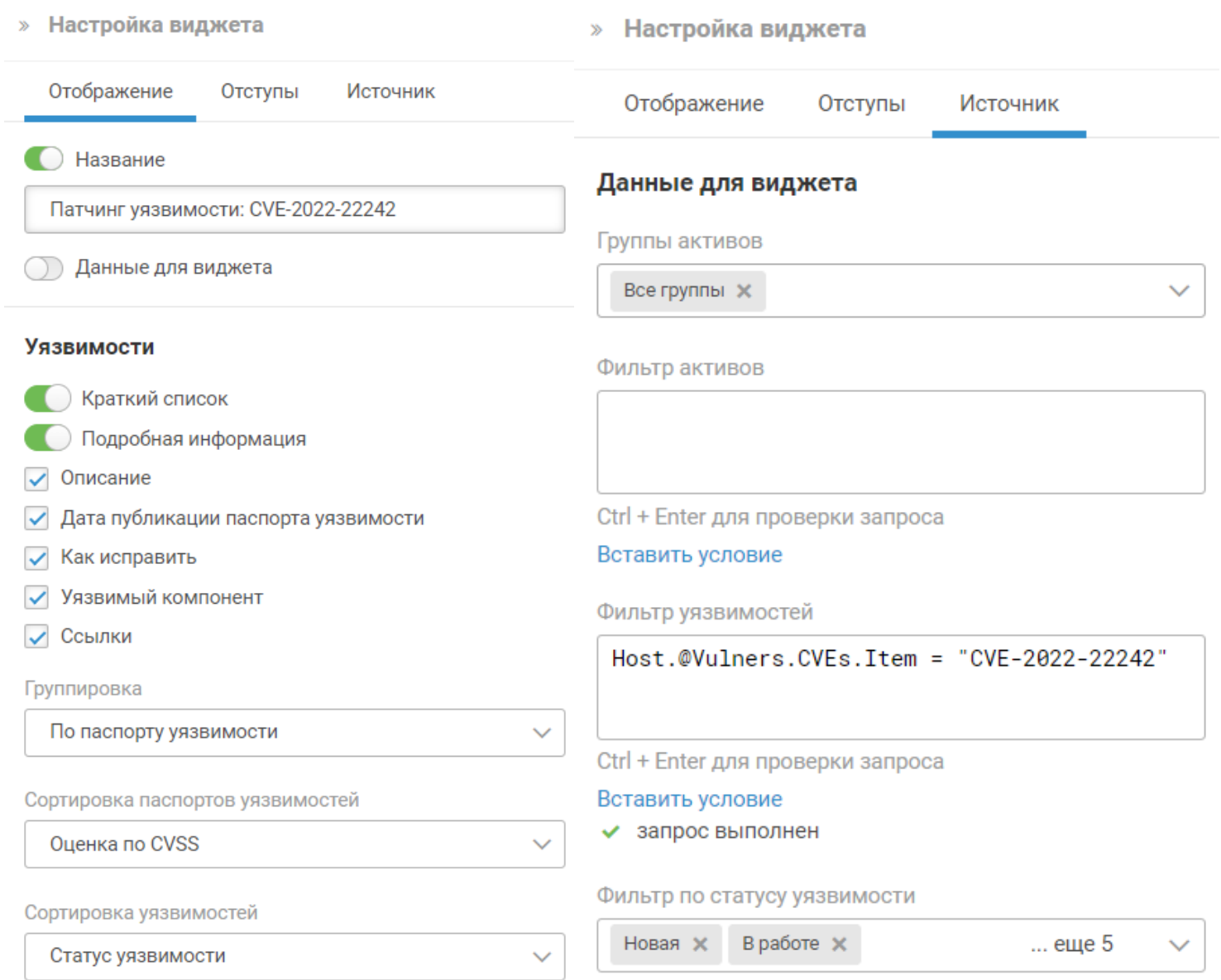
1) «Данные для виджета» -> Отключить
2) «Группировка» -> Выбираем «По паспорту уязвимости»
3) «Сортировка паспортов уязвимостей» -> Выбираем «Оценка по CVSS»
4) «Сортировка уязвимостей» -> Выбираем «Статус уязвимости»

На вкладке «Источник»

1) «Группы активов» -> Указываем группу активов, по которой хотим выпустить отчёт о наличии трендовой уязвимости, или выбираем «Все активы»
2) «Фильтр уязвимостей» -> Указываем фильтр, чтобы выбрать хосты, подверженные конкретной трендовой уязвимости:

```
Host.@Vulners.CVEs.Item = "CVE-2022-22242"
```

3) «Фильтр по статусу уязвимости» -> Выбираем все статусы


» Настройка виджета
Отображение
Отступы
Источник
Название
Патчинг уязвимости: CVE-2022-22242
Данные для виджета
Уязвимости
Краткий список
Подробная информация
Описание
Дата публикации паспорта уязвимости
Как исправить
Уязвимый компонент
Ссылки
Группировка
По паспорту уязвимости
Сортировка паспортов уязвимостей
Оценка по CVSS
Сортировка уязвимостей
Статус уязвимости
» Настройка виджета
Отображение
Отступы
Источник
Данные для виджета
Группы активов
Все группы
Фильтр активов
Ctrl + Enter для проверки запроса
Вставить условие
Фильтр уязвимостей
Host.@Vulners.CVEs.Item = "CVE-2022-22242"
Ctrl + Enter для проверки запроса
Вставить условие
запрос выполнен
Фильтр по статусу уязвимости
Новая
В работе
... еще 5