

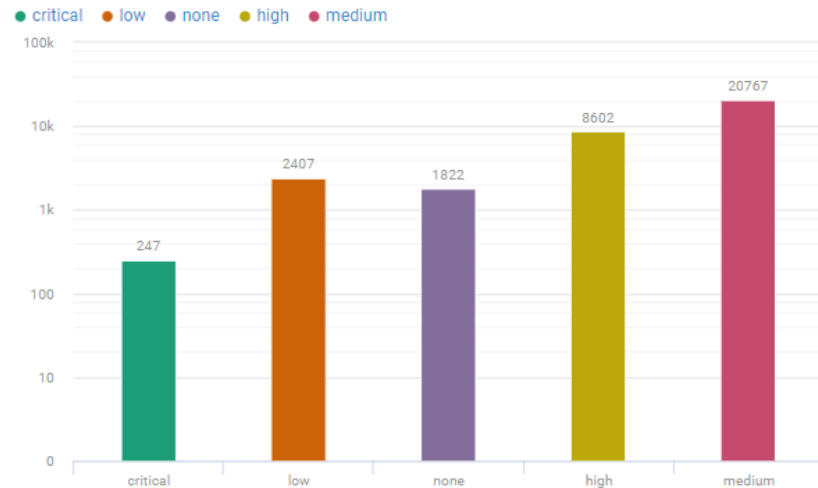
Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

1. Точечный отчёт по сканированию:	2
2. Дифференциальный отчёт.....	7
3. Динамика устранения конкретной уязвимости	25
4. Важные уязвимости за неделю: на проверку и просроченные.....	29
5. Отчёт о наличии конкретных уязвимостей (CVE, BDU, ...)	31
6. Отчёт о сбоях в процессе патч-менеджмента IT	37
7. Отчёт о «слепых зонах» в процессе патч-менеджмента IT.....	58
8. Устранение трендовых уязвимостей	70



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-ac3>

Ссылки
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-ac3>

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

■ 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-ac3>

Ссылки
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170215-ac3>

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

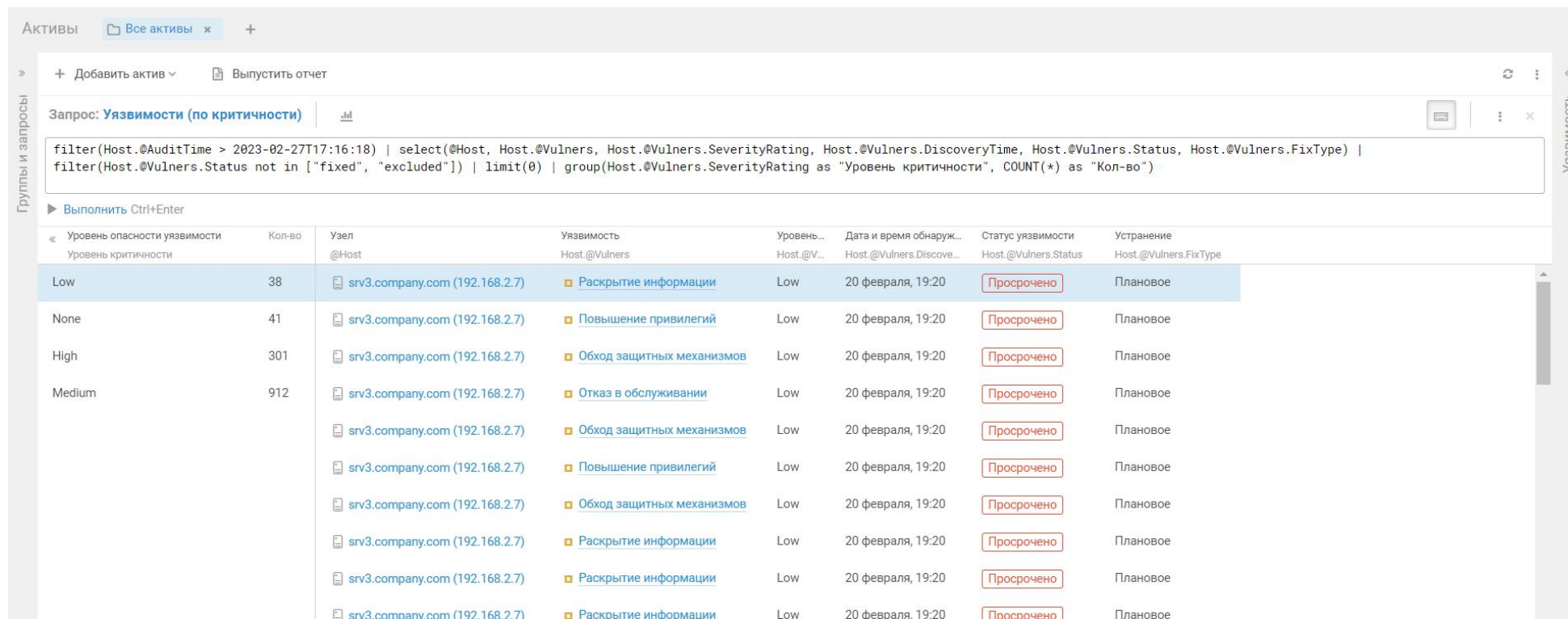
Виджет «Уязвимости (по критичности)»

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

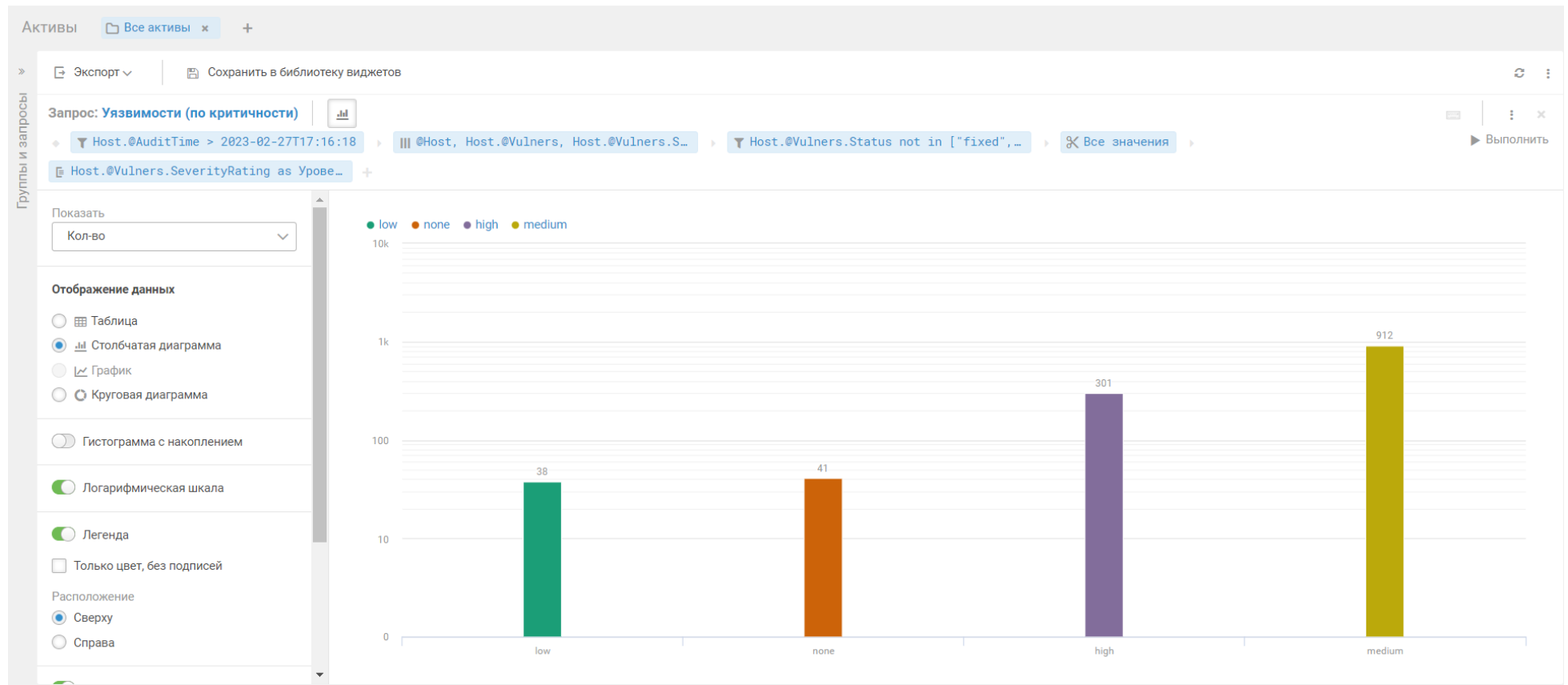


The screenshot shows the MaxPatrol VM interface. At the top, there's a tab for 'Активы' (Assets) with a sub-tab 'Все активы' (All assets). Below that, there's a search bar with the query 'Уязвимости (по критичности)'. The query is: `filter(Host.@AuditTime > 2023-02-27T17:16:18) | select(@Host, Host.@Vulners, 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")`. Below the query editor, there's a table with the following columns: 'Уровень опасности уязвимости / Уровень критичности' (Vulnerability risk level / Criticality level), 'Кол-во' (Count), 'Узел @Host' (Host), 'Уязвимость Host.@Vulners' (Vulnerability), 'Уровень... Host.@V...' (Severity), 'Дата и время обнаруж... Host.@Vulners.Discover...' (Discovery date and time), 'Статус уязвимости Host.@Vulners.Status' (Vulnerability status), and 'Устранение Host.@Vulners.FixType' (Removal). The table shows several rows of vulnerabilities, all with a status of 'Просрочено' (Expired) and a fix type of 'Плановое' (Planned).

Уровень опасности уязвимости / Уровень критичности	Кол-во	Узел @Host	Уязвимость Host.@Vulners	Уровень... Host.@V...	Дата и время обнаруж... Host.@Vulners.Discover...	Статус уязвимости Host.@Vulners.Status	Устранение Host.@Vulners.FixType
Low	38	srv3.company.com (192.168.2.7)	Раскрытие информации	Low	20 февраля, 19:20	Просрочено	Плановое
None	41	srv3.company.com (192.168.2.7)	Повышение привилегий	Low	20 февраля, 19:20	Просрочено	Плановое
High	301	srv3.company.com (192.168.2.7)	Обход защитных механизмов	Low	20 февраля, 19:20	Просрочено	Плановое
Medium	912	srv3.company.com (192.168.2.7)	Отказ в обслуживании	Low	20 февраля, 19:20	Просрочено	Плановое
		srv3.company.com (192.168.2.7)	Обход защитных механизмов	Low	20 февраля, 19:20	Просрочено	Плановое
		srv3.company.com (192.168.2.7)	Повышение привилегий	Low	20 февраля, 19:20	Просрочено	Плановое
		srv3.company.com (192.168.2.7)	Обход защитных механизмов	Low	20 февраля, 19:20	Просрочено	Плановое
		srv3.company.com (192.168.2.7)	Раскрытие информации	Low	20 февраля, 19:20	Просрочено	Плановое
		srv3.company.com (192.168.2.7)	Раскрытие информации	Low	20 февраля, 19:20	Просрочено	Плановое
		srv3.company.com (192.168.2.7)	Раскрытие информации	Low	20 февраля, 19:20	Просрочено	Плановое

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

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.

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»

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

» 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 ■ CVE-2019-0155 ■ CVE-2019-0154 CVE-2019-0154 ■ Раскрытие информации CVE-2019-11135 ■ Отказ в обслуживании CVE-2018-12207 ■ CVE-2019-14821 CVE-2019-14821 ■ CVE-2019-14835 CVE-2019-14835 ■ CVE-2019-15902 CVE-2019-15902 ■ CVE-2019-15117 CVE-2019-15117 ■ CVE-2019-15118 CVE-2019-15118 ■ Разглашение информации CVE-2019-1125 ■ CVE-2019-14283 CVE-2019-14283	0	1	0

🚩 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)	1 мар, 11:18
	Устранение: Нет политики	
	Debian Project git 1:2.1.4-2.1+deb8u2	

Сохранившиеся без изменений (за 7 дней)

Уязвимость	Количество
srv10.company.com (192.168.2.15) Igor Pavlov 7-Zip	1 0 0
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/QU361>

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	



Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

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

The screenshot shows the MaxPatrol VM interface. At the top, there's a tab labeled 'Активы' and a sub-tab 'Все активы'. Below that, there's a search bar with the query 'Динамика уязвимостей (по критичности)'. The query is displayed in a text area: `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)`. Below the query, there's a button 'Выполнить Ctrl+Enter'. The main part of the interface is a table with the following columns: 'Дата и время ...', 'Уровень опа...', 'Кол-во', 'Узел', 'Уязвимость', 'Уровень опа...', and 'Дата и время дл...'. The table contains several rows of data, including vulnerability details for 'pc1.company.com (192.168.0.64)' such as 'Повышение привилегий' and 'Разглашение информации'.

Дата и время ...	Уровень опа...	Кол-во	Узел	Уязвимость	Уровень опа...	Дата и время дл...
Время	Критичность		@Host	Host.@Vulners	Host.@Vulner...	Host.@Time
01 марта, 23:59	Medium	35470	pc1.company.com (192.168.0.64)	Повышение привилегий	Medium	01 марта, 23:59
01 марта, 23:59	None	2383	pc1.company.com (192.168.0.64)	Разглашение информации	Medium	01 марта, 23:59
01 марта, 23:59	Critical	678	pc1.company.com (192.168.0.64)	Разглашение информации	Medium	01 марта, 23:59
01 марта, 23:59	Low	5550	pc1.company.com (192.168.0.64)	Обход функций безопасности ASLR	Medium	01 марта, 23:59
01 марта, 23:59	High	15000	pc1.company.com (192.168.0.64)	Повышение привилегий	Medium	01 марта, 23:59
02 марта, 23:59	Medium	35470	pc1.company.com (192.168.0.64)	Повышение привилегий	Medium	01 марта, 23:59

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

Запрос: **Динамика уязвимостей (по критичности)**

6 д, 1 д, endofday()

Host, Host.@Vulners, Host.@Vul

Данные за период

Длительность: 6 дней

Детализация: 1 день

Окончание: Конец дня

Будут показаны данные с 2 марта, 23:59 по 8 марта, 23:59 с детализацией 1 день

Выполнить (Ctrl + Enter) **Добавить** Отмена

Переходим в режим создания виджета нажатием соответствующей иконки:

Активы Все активы +

Экспорт Сохранить в библиотеку виджетов

Запрос: **Динамика уязвимостей (по критичности)**

6 д, 1 д, endofday() Host, Host.@Vulners, Host.@Vulners.S... Host.@Vulners Все значения Host.@Time as Время, Host.@Vulners.Se... Время ASC Выполнить

Показать: Кол-во

Отображение данных

- Таблица
- Столбчатая диаграмма
- График
- Круговая диаграмма

Показать сумму по столбцу

Показать сумму по строке

Критичность	1 марта, 23:59	2 марта, 23:59	3 марта, 23:59	4 марта, 23:59	5 марта, 23:59	6 марта, 23:59
medium	35470	35470	35470	35470	35470	35470
none	2383	2383	2383	2383	2380	2380
critical	678	678	678	678	678	678
low	5550	5550	5550	5550	5550	5550
high	15000	15000	15000	15000	15003	15003

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

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

Активы Все активы x +

+ Добавить актив Выпустить отчет

Запрос: **Общая статистика по узлам**

```
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() - 9d) | 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.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)
```

Выполнить Ctrl+Enter

Узел @Host	Устранённые уязвимости	Новые уязвимости	Сохранившиеся без изменений	Сохранившиеся с изменениями
switch3.company.com (192.168.0.233)	null	null	12	null
switch2.company.com (192.168.0.211)	null	null	12	null
srv9.company.com (192.168.0.14)	null	1	1152	1
srv7.company.com (192.168.2.12)	null	2	1167	3
srv6.company.com (192.168.0.11)	null	null	1090	null
srv3.company.com (192.168.2.7)	null	null	1259	null
srv2.company.com (192.168.0.6)	null	null	106	null
srv13.company.com (192.168.2.8)	null	null	3476	null

Всего 44 записи, выбрана 1 запись (1 актив)

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

Переходим в режим создания виджета нажатием соответствующей иконки:

Экспорт | Сохранить в библиотеку виджетов

Запрос: **Общая статистика по узлам**

select(@Host, Host.@Vulners, Host.@Vu... | select(@Host, Host.@Vulners, Host.@Vu... | select(@Host, Host.@Vulners, Host.@Vu... | select(@Host, Host.@Vulners, Host.@Vu... | @Host, Q.Fixed as Устранённые уязвимо... | "Устранённые уязвимости" != null or "... | @Host DESC

Выполнить

Группы и запросы

Отображение данных

- Таблица
- Столбчатая диаграмма
- График
- Круговая диаграмма

@Host	Устранённые уязвимости	Новые уязвимости	Сохранившиеся без изменений	Сохранившиеся с изменениями
switch3.company.com (192.168...	null	null	12	null
switch2.company.com (192.168...	null	null	12	null
srv9.company.com (192.168.0.14)	null	1	1152	1
srv7.company.com (192.168.2.12)	null	2	1167	3
srv6.company.com (192.168.0.11)	null	null	1090	null
srv3.company.com (192.168.2.7)	null	null	1259	null
srv2.company.com (192.168.0.6)	null	null	106	null
srv13.company.com (192.168.2.8)	null	null	3476	null
srv12.company.com (192.168.0...	null	7	6018	7
srv11.company.com (192.168.2...	null	8	811	9
srv10.company.com (192.168.2...	null	null	2684	null
router9.company.com (192.168.0...	null	null	16	null

Всего 44 строки, выбрано 0 строк

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»

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

» 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 x

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 x

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»

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

» 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»

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

» 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»

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

» 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

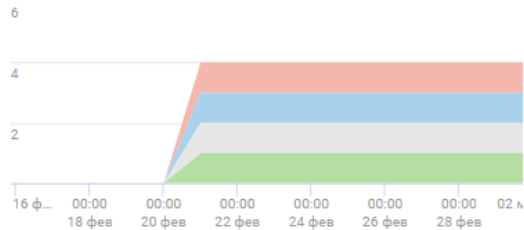
актуальные уязвимости

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
Трендовая	9
Удаленно	0
Есть исправление	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».

Создание задачи Все шаблоны ▾ ✕


Без шаблона

Важные уязвимости

🛡️ Важные уязвимости за неделю: на проверку и просроченные

🛡️ Важные уязвимости за неделю: устраненные

🛡️ Важные уязвимости, которые еще актуальны

🛡️ Важные уязвимости: за неделю и еще актуальные

🛡️ Уязвимость Zerologon и динамика ее устранения

Другие

🛡️ Отчеты по активам и инцидентам

Далее Отмена

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

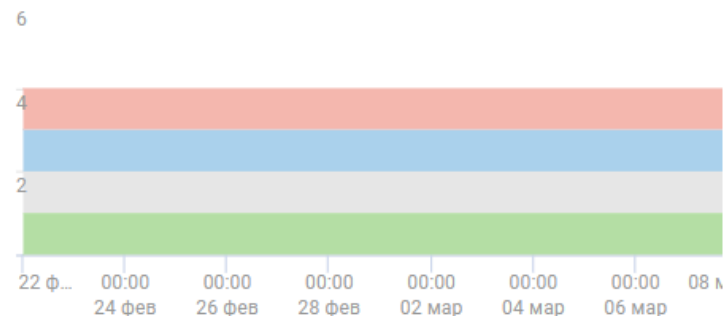
актуальные уязвимости

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

- 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».

The screenshot displays the configuration interface for a widget in MaxPatrol VM. It is divided into three main sections:

- Настройка виджета (Widget Settings):** This section is split into two identical panels. Each panel has tabs for 'Отображение' (Display), 'Отступы' (Margins), and 'Источник' (Source). Under 'Источник', there are three fields:
 - Группы активов (Asset Groups):** A dropdown menu set to 'Все группы' (All groups).
 - Фильтр активов (Asset Filter):** An empty text input field.
 - Фильтр уязвимостей (Vulnerability Filter):** A text input field containing the query: `compact(Host.@Vulners.CVEs) intersect ["CVE-2022-41076"]` in the left panel, and `Host.@Vulners.Ids in ["BDU:2023-00755"]` in the right panel.
- Данные за период (Data Period):** This section contains:
 - Длительность (Duration):** A dropdown menu set to '2' weeks.
 - Детализация (Granularity):** A dropdown menu set to '1' day.
 - Окончание (End):** A text input field containing the query: `endofday() - 1d`.
- Отображение данных (Data Display):** This section contains:
 - Отображение (Display):** A dropdown menu set to 'Уязвимости' (Vulnerabilities).
 - Чекбоксы (Checkboxes):** Three checkboxes are checked: 'Актуальные' (Current), 'Исключены' (Excluded), and 'Устранены' (Resolved).

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

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

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

» Настройка виджета

Отображение Отступы **Источник**

Данные для виджета

Группы активов
Все группы x

Фильтр активов

Ctrl + Enter для проверки запроса
[Вставить условие](#)

Фильтр уязвимостей
`compact(Host.@Vulners.CVEs) intersect ["CVE-2022-41076"]`

Ctrl + Enter для проверки запроса
[Вставить условие](#)

Фильтр по статусу уязвимости
Новая x В работе x ... еще 4

» Настройка виджета

Отображение Отступы **Источник**

Данные для виджета

Группы активов
Все группы x

Фильтр активов

Ctrl + Enter для проверки запроса
[Вставить условие](#)

Фильтр уязвимостей
`Host.@Vulners.Ids in ["BDU:2023-00755"]`

Ctrl + Enter для проверки запроса
[Вставить условие](#)

Фильтр по статусу уязвимости
Новая x В работе x ... еще 4

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: потребовавшиеся 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».

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

Создание задачи Все шаблоны ▾ ✕


Без шаблона

Важные уязвимости

🛡️ Важные уязвимости за неделю: на проверку и просроченные

🛡️ Важные уязвимости за неделю: устраненные

🛡️ Важные уязвимости, которые еще актуальны

🛡️ Важные уязвимости: за неделю и еще актуальные

🛡️ Уязвимость Zerologon и динамика ее устранения

Другие

🛡️ Отчеты по активам и инцидентам

Далее Отмена

Все параметры отчёта можно оставить по умолчанию.

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

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

- Уязвимость CVE-2023-0512** CVE-2023-0512 Уязвимости не обнаружены
Уязвимость текстового редактора Vim связана с ошибкой деления на ноль в функции 'smoothscroll' при малых размерах окна. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать сбой программы
- Повышение привилегий** CVE-2023-21823

4	0	1
---	---	---

Уязвимость, связанная с повышением привилегий, позволяет злоумышленникам оказать воздействие на систему.
- Уязвимость CVE-2023-0687** CVE-2023-0687 Уязвимости не обнаружены
Уязвимость библиотеки системных вызовов и основных функций GNU C Library(glibc) связана с переполнением буфера в функции __monstartup файла gmon.c компонента Call Graph Monitor. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, переполнить буфер и получить доступ к конфиденциальным данным

Список уязвимостей

Уязвимость	Количество			
Повышение привилегий Microsoft Windows	<table border="1"><tr><td>4</td><td>0</td><td>1</td></tr></table>	4	0	1
4	0	1		
Повышение привилегий Microsoft Windows				
Трендовая Есть эксплойт Есть исправление	<table border="1"><tr><td>4</td><td>0</td><td>1</td></tr></table>	4	0	1
4	0	1		
Уязвимость, связанная с повышением привилегий, позволяет злоумышленникам оказать воздействие на систему.				
Дата публикации 14 февраля, 03:00				
Как исправить Используйте рекомендации производителя: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21823				
Статус	Уязвимость на активе	Обнаружена		
Исправляется	srv10.company.com (192.168.2.15)	21 фев, 00:57		
16 мар, 13:29 Важная Устранение: Плановое				

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»

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

» 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

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

» 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 ×

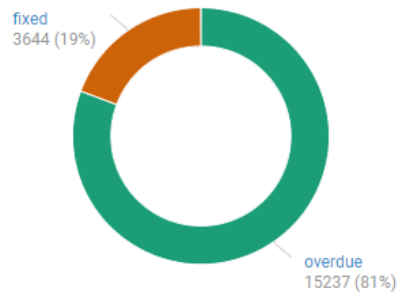
В работе ×

... еще 5

6. Отчёт о сбоях в процессе патч-менеджмента IT

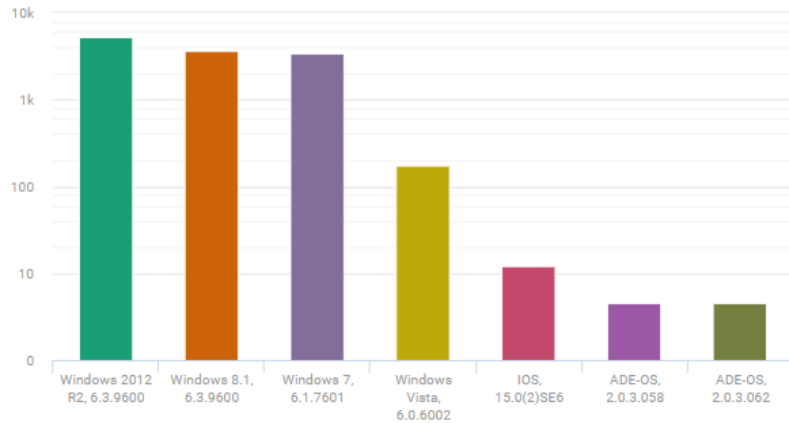
Уязвимости: Просроченные | Устранённые

overdue fixed



(II) Уязвимости ОС на активах

Windows 2012 R2, 6.3... Windows 8.1, 6.3.9600 Windows 7, 6.1.7601
 Windows Vista, 6.0.6002 IOS, 15.0(2)SE6 ADE-OS, 2.0.3.058 ADE-OS, 2.0.3.062

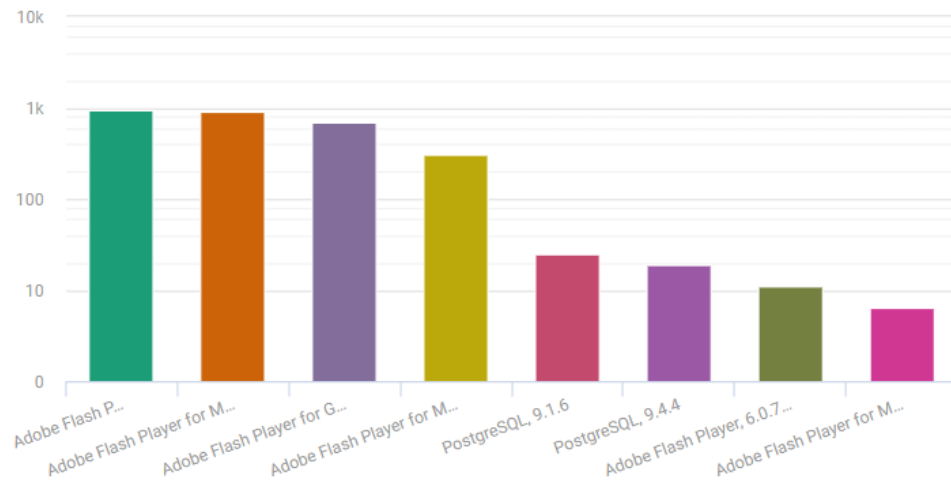


(II) Уязвимости ОС на активах (по хосту)

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

- Adobe Flash Player for ...
- Adobe Flash Player for ...
- Adobe Flash Player for ...
- Adobe Flash Player for ...
- PostgreSQL, 9.1.6
- PostgreSQL, 9.4.4
- Adobe Flash Player, 6.0...
- Adobe Flash Player for ...




(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:

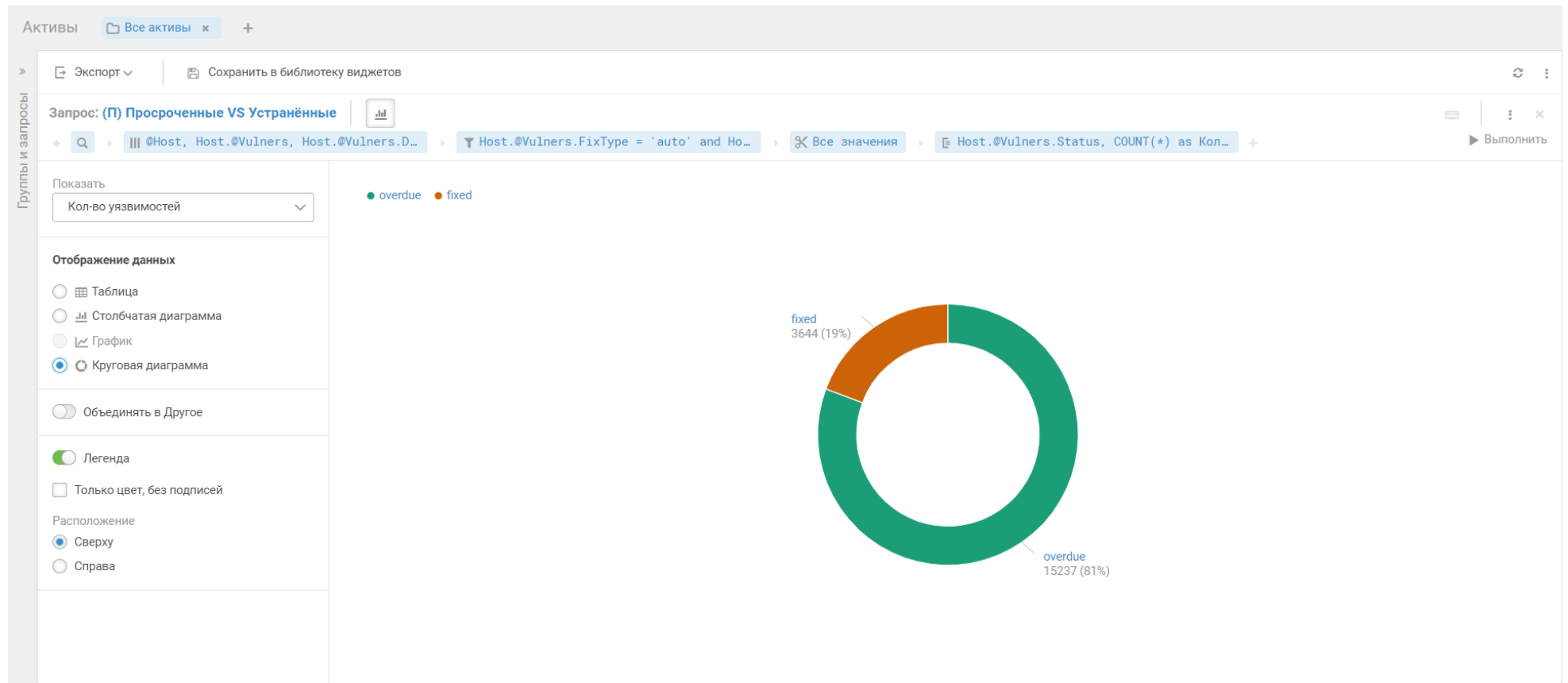
```
select(@Host, Host.@Vulners, Host.@Vulners.DiscoveryTime, Host.@Vulners.Status, Host.@Vulners.FixType) | filter(Host.@Vulners.FixType = 'auto' and Host.@Vulners.Status in ['overdue', 'fixed']) | limit(0) | group(Host.@Vulners.Status, COUNT(*) as "Кол-во уязвимостей")
```

The screenshot shows the MaxPatrol VM interface. At the top, there's a search bar with the query: `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")`. Below the query, there's a table with columns: Статус уязвимости, Кол-во уязвимостей, Узел, Уязвимость, Дата и время обнаруж..., Статус уязвимости, and Устранение. The table shows two main rows: 'Просрочено' with 15237 vulnerabilities and 'Устранена' with 3644 vulnerabilities. Below these, a list of specific vulnerabilities is shown, including 'Использование после освобождения', 'Смещение типов', 'Разыменованное нулевого указателя', 'Раскрытие информации', 'Удаленное выполнение кода', and 'Повышение привилегий'. The status for all these is 'Просрочено' and the fix type is 'Плановое'.

Статус уязвимости	Кол-во уязвимостей	Узел	Уязвимость	Дата и время обнаруж...	Статус уязвимости	Устранение
Просрочено	15237	pc14.company.com (192.168.0.100)	Использование после освобождения	20 февраля, 19:18	Просрочено	Плановое
Устранена	3644	pc14.company.com (192.168.0.100)	Смещение типов	20 февраля, 19:18	Просрочено	Плановое
		pc14.company.com (192.168.0.100)	Разыменованное нулевого указате...	20 февраля, 19:18	Просрочено	Плановое
		pc14.company.com (192.168.0.100)	Использование после освобождения	20 февраля, 19:18	Просрочено	Плановое
		pc14.company.com (192.168.0.100)	Смещение типов	20 февраля, 19:18	Просрочено	Плановое
		pc14.company.com (192.168.0.100)	Разыменованное нулевого указате...	20 февраля, 19:18	Просрочено	Плановое
		srv6.company.com (192.168.0.11)	Раскрытие информации	20 февраля, 19:18	Просрочено	Плановое
		srv6.company.com (192.168.0.11)	Удаленное выполнение кода	20 февраля, 19:18	Просрочено	Плановое
		srv6.company.com (192.168.0.11)	Повышение привилегий	21 февраля, 00:57	Просрочено	Плановое
		srv6.company.com (192.168.0.11)	Удаленное выполнение кода	20 февраля, 19:18	Просрочено	Плановое
		srv6.company.com (192.168.0.11)	Повышение привилегий	20 февраля, 19:18	Просрочено	Плановое

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

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.

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

Виджет: «(П) Уязвимости ОС на активах»

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

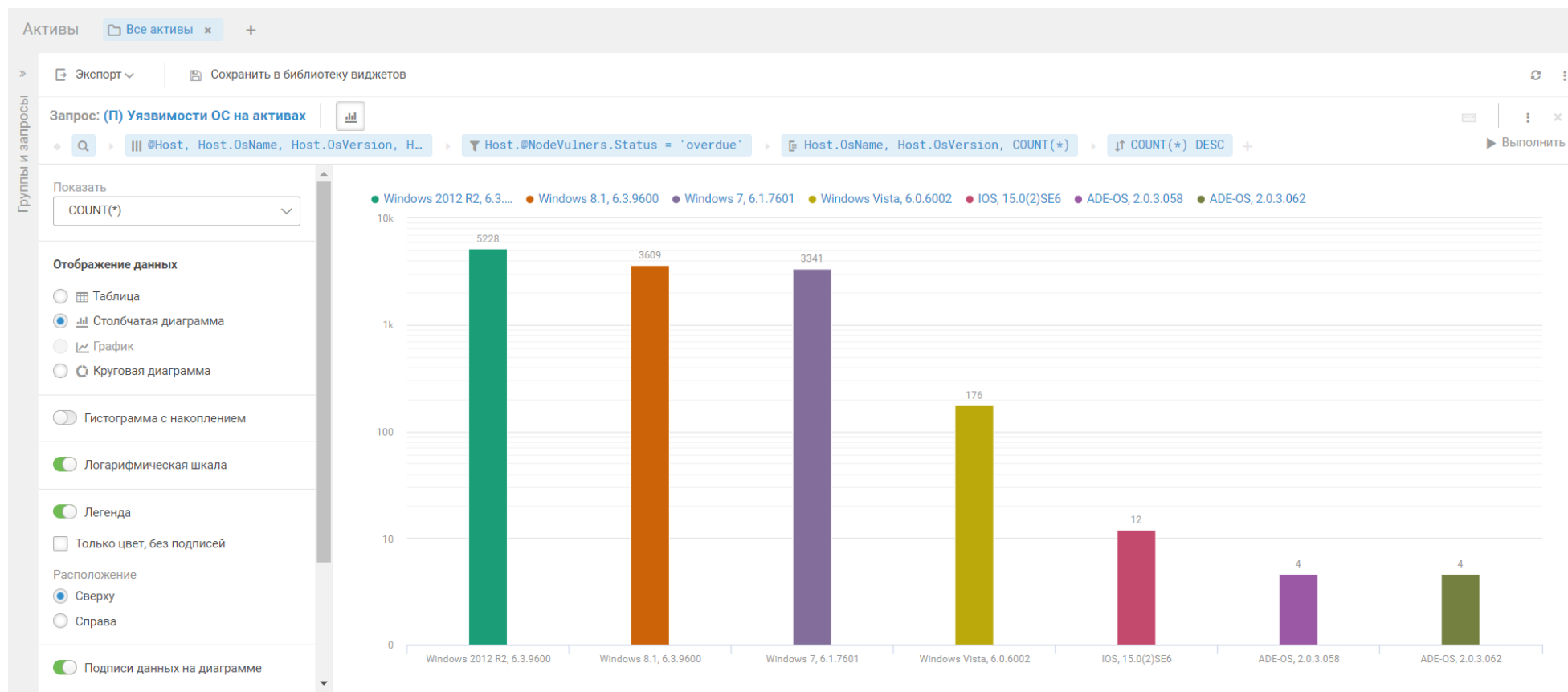
Вставляем и выполняем следующий запрос:

```
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)
```

Операционная с... Host.OsName	Версия опера... Host.OsVersion	COUNT(...)	Узел @Host	Операционная сист... Host.OsName	Версия оп... Host.OsVe...	Уязвимость Host.@NodeVulners	Дата и время обнару... Host.@NodeVulners.Di...	Статус уязвимости Host.@NodeVulners.St...	Устранение Host.@NodeVulners.Fi...	Метки уязвимости Host.@NodeVulners.Ta...
Windows 2012 R2	6.3.9600	5228	srv6.company.com (192.168.0.11)	Windows 2012 R2	6.3.9600	Раскрытие информации	20 февраля, 19:18	Просрочено	Плановое	null
Windows 8.1	6.3.9600	3609	srv6.company.com (192.168.0.11)	Windows 2012 R2	6.3.9600	Удаленное выполнение кода	20 февраля, 19:18	Просрочено	Плановое	null
Windows 7	6.1.7601	3341	srv6.company.com (192.168.0.11)	Windows 2012 R2	6.3.9600	Повышение привилегий	21 февраля, 00:57	Просрочено	Плановое	null
Windows Vista	6.0.6002	176	srv6.company.com (192.168.0.11)	Windows 2012 R2	6.3.9600	Удаленное выполнение кода	20 февраля, 19:18	Просрочено	Плановое	null
IOS	15.0(2)SE6	12	srv6.company.com (192.168.0.11)	Windows 2012 R2	6.3.9600	Повышение привилегий	20 февраля, 19:18	Просрочено	Плановое	null
ADE-OS	2.0.3.058	4	srv6.company.com (192.168.0.11)	Windows 2012 R2	6.3.9600	Удаленное выполнение кода	20 февраля, 19:18	Просрочено	Плановое	null
ADE-OS	2.0.3.062	4	srv6.company.com (192.168.0.11)	Windows 2012 R2	6.3.9600	Повышение привилегий	20 февраля, 19:18	Просрочено	Плановое	null
			srv6.company.com (192.168.0.11)	Windows 2012 R2	6.3.9600	Удаленное выполнение кода	20 февраля, 19:18	Просрочено	Плановое	null
			srv6.company.com (192.168.0.11)	Windows 2012 R2	6.3.9600	Раскрытие информации	20 февраля, 19:18	Просрочено	Плановое	null
			srv6.company.com (192.168.0.11)	Windows 2012 R2	6.3.9600	Повышение привилегий	20 февраля, 19:18	Просрочено	Плановое	null
			srv6.company.com (192.168.0.11)	Windows 2012 R2	6.3.9600	Удаленное выполнение кода	20 февраля, 19:18	Просрочено	Плановое	null

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

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.

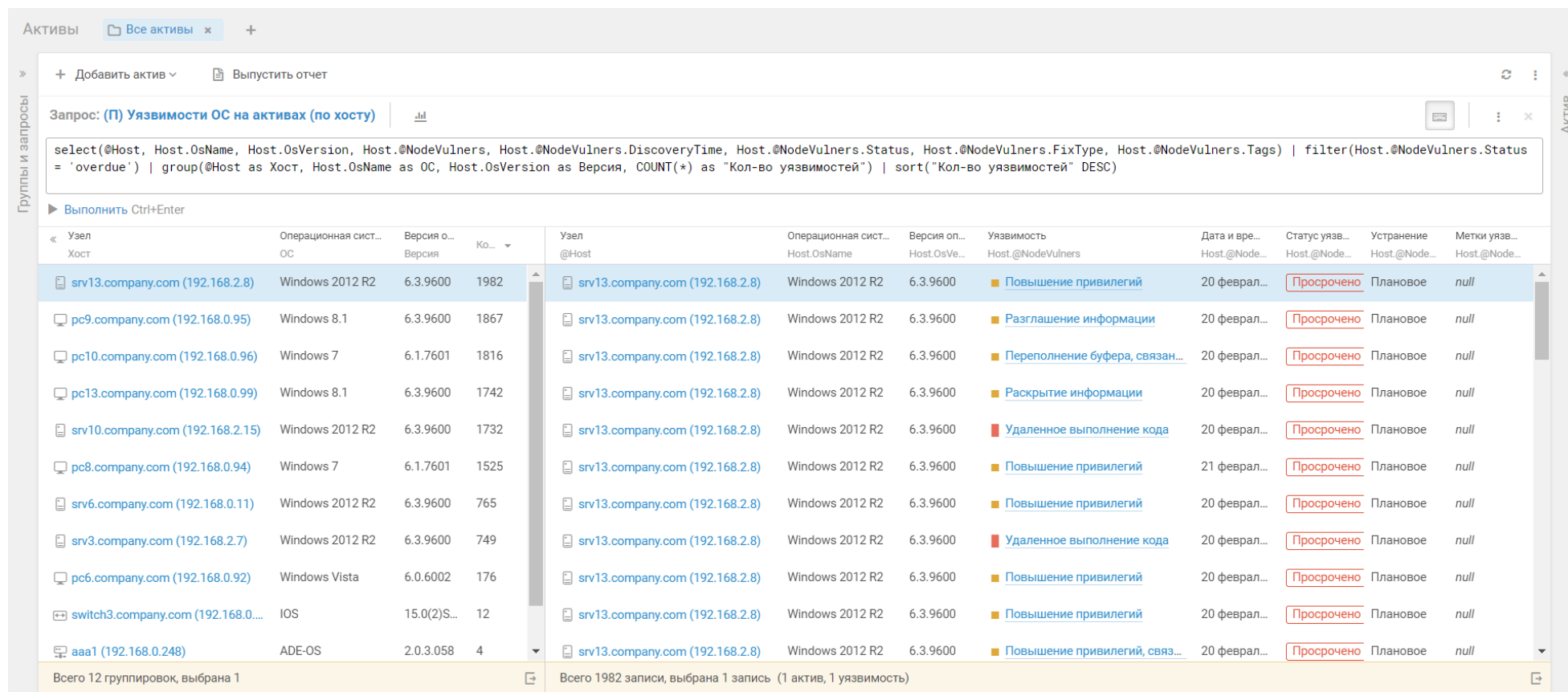
Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

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)
```

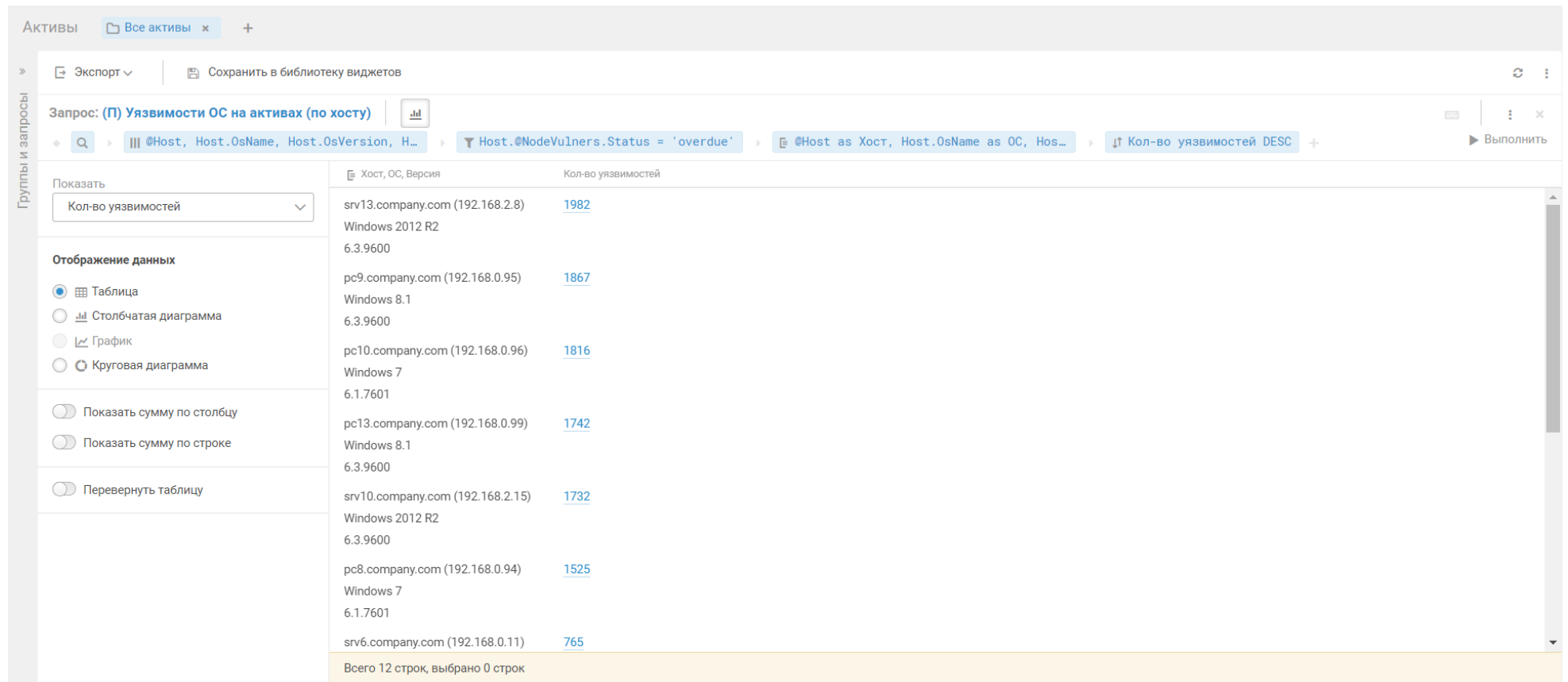


The screenshot shows the MaxPatrol VM interface. At the top, there's a search bar with the query: `select(@Host, Host.OsName, Host.OsVersion, Host.@NodeVulners, Host.@NodeVulners.DiscoveryTime, Host.@NodeVulners.Status, Host.@NodeVulners.FixType, Host.@NodeVulners.Tags) | filter(Host.@NodeVulners.Status = 'overdue') | group(@Host as Хост, Host.OsName as ОС, Host.OsVersion as Версия, COUNT(*) as "Кол-во уязвимостей") | sort("Кол-во уязвимостей" DESC)`. Below the query editor is a table with columns for Host, OS, Version, Count, Vulnerability Name, Date, Status, Fix Type, and Tags. The table is sorted by the number of vulnerabilities in descending order.

Узел	Операционная сист...	Версия о...	Ко...	Узел	Операционная сист...	Версия оп...	Уязвимость	Дата и вре...	Статус уязв...	Устранение	Метки уязв...
Хост	ОС	Версия	Ко...	@Host	Host.OsName	Host.OsVe...	Host.@NodeVulners	Host.@Node...	Host.@Node...	Host.@Node...	Host.@Node...
srv13.company.com (192.168.2.8)	Windows 2012 R2	6.3.9600	1982	srv13.company.com (192.168.2.8)	Windows 2012 R2	6.3.9600	Повышение привилегий	20 феврал...	Просрочено	Плановое	null
pc9.company.com (192.168.0.95)	Windows 8.1	6.3.9600	1867	srv13.company.com (192.168.2.8)	Windows 2012 R2	6.3.9600	Разглашение информации	20 феврал...	Просрочено	Плановое	null
pc10.company.com (192.168.0.96)	Windows 7	6.1.7601	1816	srv13.company.com (192.168.2.8)	Windows 2012 R2	6.3.9600	Переполнение буфера, связан...	20 феврал...	Просрочено	Плановое	null
pc13.company.com (192.168.0.99)	Windows 8.1	6.3.9600	1742	srv13.company.com (192.168.2.8)	Windows 2012 R2	6.3.9600	Раскрытие информации	20 феврал...	Просрочено	Плановое	null
srv10.company.com (192.168.2.15)	Windows 2012 R2	6.3.9600	1732	srv13.company.com (192.168.2.8)	Windows 2012 R2	6.3.9600	Удаленное выполнение кода	20 феврал...	Просрочено	Плановое	null
pc8.company.com (192.168.0.94)	Windows 7	6.1.7601	1525	srv13.company.com (192.168.2.8)	Windows 2012 R2	6.3.9600	Повышение привилегий	21 феврал...	Просрочено	Плановое	null
srv6.company.com (192.168.0.11)	Windows 2012 R2	6.3.9600	765	srv13.company.com (192.168.2.8)	Windows 2012 R2	6.3.9600	Повышение привилегий	20 феврал...	Просрочено	Плановое	null
srv3.company.com (192.168.2.7)	Windows 2012 R2	6.3.9600	749	srv13.company.com (192.168.2.8)	Windows 2012 R2	6.3.9600	Удаленное выполнение кода	20 феврал...	Просрочено	Плановое	null
pc6.company.com (192.168.0.92)	Windows Vista	6.0.6002	176	srv13.company.com (192.168.2.8)	Windows 2012 R2	6.3.9600	Повышение привилегий	20 феврал...	Просрочено	Плановое	null
switch3.company.com (192.168.0...	IOS	15.0(2)S...	12	srv13.company.com (192.168.2.8)	Windows 2012 R2	6.3.9600	Повышение привилегий	20 феврал...	Просрочено	Плановое	null
aaa1 (192.168.0.248)	ADE-OS	2.0.3.058	4	srv13.company.com (192.168.2.8)	Windows 2012 R2	6.3.9600	Повышение привилегий, связ...	20 феврал...	Просрочено	Плановое	null

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

Переходим в режим создания виджета нажатием соответствующей иконки:



Активы Все активы x +

Экспорт v Сохранить в библиотеку виджетов

Запрос: (П) Уязвимости ОС на активах (по хосту)

Host.@NodeVulnners.Status = 'overdue' @Host as Хост, Host.OsName as ОС, Hos... Кол-во уязвимостей DESC + Выполнить

Показать: Кол-во уязвимостей

Отображение данных

- Таблица
- Столбчатая диаграмма
- График
- Круговая диаграмма

Показать сумму по столбцу

Показать сумму по строке

Перевернуть таблицу

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)	765

Всего 12 строк, выбрано 0 строк

Сохраняем получившийся виджет в библиотеку виджетов нажатием соответствующей кнопки.

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

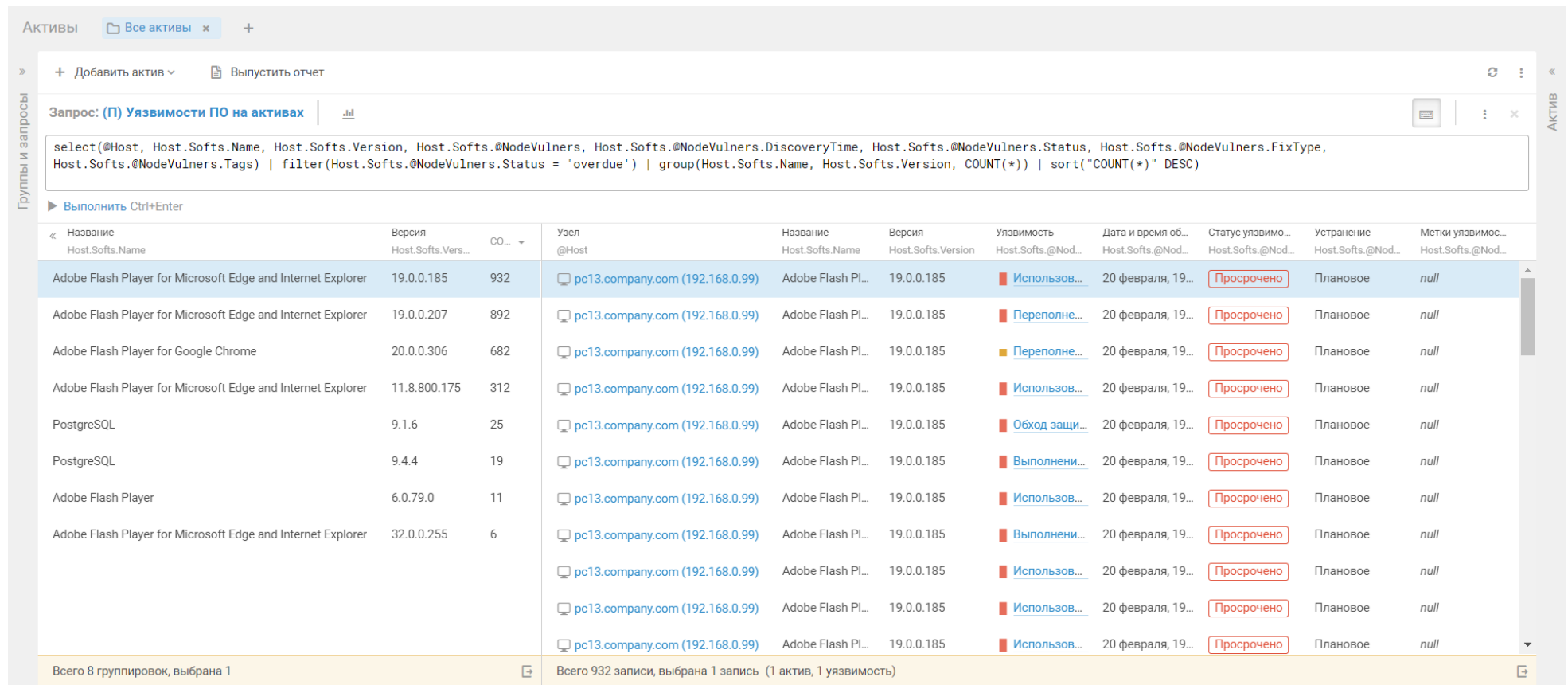
Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

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)
```



The screenshot shows the MaxPatrol VM interface. At the top, there's a header with 'Активы' and a tab 'Все активы'. Below that, there's a search bar with the query '(П) Уязвимости ПО на активах'. The query editor contains the following query:

```
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)
```

Below the query editor, there's a table with the following columns: Название, Версия, CO..., Узел, Название, Версия, Уязвимость, Дата и время об..., Статус уязвимо..., Устранение, and Метки уязвимос... The table contains 8 rows of data, each representing a software vulnerability. The first row is highlighted in blue.

Название	Версия	CO...	Узел	Название	Версия	Уязвимость	Дата и время об...	Статус уязвимо...	Устранение	Метки уязвимос...
Adobe Flash Player for Microsoft Edge and Internet Explorer	19.0.0.185	932	pc13.company.com (192.168.0.99)	Adobe Flash Pl...	19.0.0.185	Используй...	20 февраля, 19...	Просрочено	Плановое	null
Adobe Flash Player for Microsoft Edge and Internet Explorer	19.0.0.207	892	pc13.company.com (192.168.0.99)	Adobe Flash Pl...	19.0.0.185	Переполне...	20 февраля, 19...	Просрочено	Плановое	null
Adobe Flash Player for Google Chrome	20.0.0.306	682	pc13.company.com (192.168.0.99)	Adobe Flash Pl...	19.0.0.185	Переполне...	20 февраля, 19...	Просрочено	Плановое	null
Adobe Flash Player for Microsoft Edge and Internet Explorer	11.8.800.175	312	pc13.company.com (192.168.0.99)	Adobe Flash Pl...	19.0.0.185	Используй...	20 февраля, 19...	Просрочено	Плановое	null
PostgreSQL	9.1.6	25	pc13.company.com (192.168.0.99)	Adobe Flash Pl...	19.0.0.185	Обход защи...	20 февраля, 19...	Просрочено	Плановое	null
PostgreSQL	9.4.4	19	pc13.company.com (192.168.0.99)	Adobe Flash Pl...	19.0.0.185	Выполни...	20 февраля, 19...	Просрочено	Плановое	null
Adobe Flash Player	6.0.79.0	11	pc13.company.com (192.168.0.99)	Adobe Flash Pl...	19.0.0.185	Используй...	20 февраля, 19...	Просрочено	Плановое	null
Adobe Flash Player for Microsoft Edge and Internet Explorer	32.0.0.255	6	pc13.company.com (192.168.0.99)	Adobe Flash Pl...	19.0.0.185	Выполни...	20 февраля, 19...	Просрочено	Плановое	null

At the bottom of the table, there's a summary: 'Всего 8 группировок, выбрана 1' and 'Всего 932 записи, выбрана 1 запись (1 актив, 1 уязвимость)'.

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

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)
```

The screenshot shows the MaxPatrol VM interface. At the top, there's a search bar with the query: `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)`. Below the query editor is a table with columns: Узел, Название, Версия, Кол-во, Узел, Название, Версия, Уязвимо..., Дата и вр..., Статус уя..., Устранен..., Метки уя... The table displays 9 rows of grouped data for various hosts and software versions. The status of vulnerabilities is shown as 'Исполнено', 'Перепроверено', or 'Выполнено'. The bottom status bar indicates: 'Всего 9 группировок, выбрана 1' and 'Всего 932 записи, выбрана 1 запись (1 актив, 1 уязвимость)'.

Узел	Название	Версия	Кол-во	Узел	Название	Версия	Уязвимо...	Дата и вр...	Статус уя...	Устранен...	Метки уя...
pc13.company.com (192.168.0.99)	Adobe Flash Player for Microsoft Edge and Internet Explorer	19.0.0.185	932	pc13.company.com (192.168.0.99)	Adobe Fl...	19.0.0.185	Испол...	20 февр...	Просрочен	Плановое	null
pc12.company.com (192.168.0.98)	Adobe Flash Player for Microsoft Edge and Internet Explorer	19.0.0.207	892	pc13.company.com (192.168.0.99)	Adobe Fl...	19.0.0.185	Пере...	20 февр...	Просрочен	Плановое	null
pc8.company.com (192.168.0.94)	Adobe Flash Player for Google Chrome	20.0.0.306	682	pc13.company.com (192.168.0.99)	Adobe Fl...	19.0.0.185	Пере...	20 февр...	Просрочен	Плановое	null
srv13.company.com (192.168.2.8)	Adobe Flash Player for Microsoft Edge and Internet Explorer	11.8.800.175	156	pc13.company.com (192.168.0.99)	Adobe Fl...	19.0.0.185	Испол...	20 февр...	Просрочен	Плановое	null
pc9.company.com (192.168.0.95)	Adobe Flash Player for Microsoft Edge and Internet Explorer	11.8.800.175	156	pc13.company.com (192.168.0.99)	Adobe Fl...	19.0.0.185	Обхо...	20 февр...	Просрочен	Плановое	null
srv12.company.com (192.168.0.17)	PostgreSQL	9.1.6	25	pc13.company.com (192.168.0.99)	Adobe Fl...	19.0.0.185	Выпо...	20 февр...	Просрочен	Плановое	null
srv6.company.com (192.168.0.11)	PostgreSQL	9.4.4	19	pc13.company.com (192.168.0.99)	Adobe Fl...	19.0.0.185	Испол...	20 февр...	Просрочен	Плановое	null
pc3.company.com (192.168.0.76)	Adobe Flash Player	6.0.79.0	11	pc13.company.com (192.168.0.99)	Adobe Fl...	19.0.0.185	Выпо...	20 февр...	Просрочен	Плановое	null
pc14.company.com (192.168.0.100)	Adobe Flash Player for Microsoft Edge and Internet Explorer	32.0.0.255	6	pc13.company.com (192.168.0.99)	Adobe Fl...	19.0.0.185	Испол...	20 февр...	Просрочен	Плановое	null
				pc13.company.com (192.168.0.99)	Adobe Fl...	19.0.0.185	Испол...	20 февр...	Просрочен	Плановое	null
				pc13.company.com (192.168.0.99)	Adobe Fl...	19.0.0.185	Испол...	20 февр...	Просрочен	Плановое	null

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

Переходим в режим создания виджета нажатием соответствующей иконки:

Активы Все активы x +

Экспорт Сохранить в библиотеку виджетов

Запрос: (П) Уязвимости ПО на активах (по хостам)

Q @Host, Host.Softs.Name, Host.Softs.Ve... Host.Softs.@NodeVulners.Status = 'ove... @Host, Host.Softs.Name, Host.Softs.Ve... Кол-во уязвимостей DESC + Выполнить

Показать: Кол-во уязвимостей

Отображение данных

- Таблица
- Столбчатая диаграмма
- График
- Круговая диаграмма

Показать сумму по столбцу

Показать сумму по строке

Перевернуть таблицу

@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)	19

Всего 9 строк, выбрано 0 строк

Сохраняем получившийся виджет в библиотеку виджетов нажатием соответствующей кнопки.

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

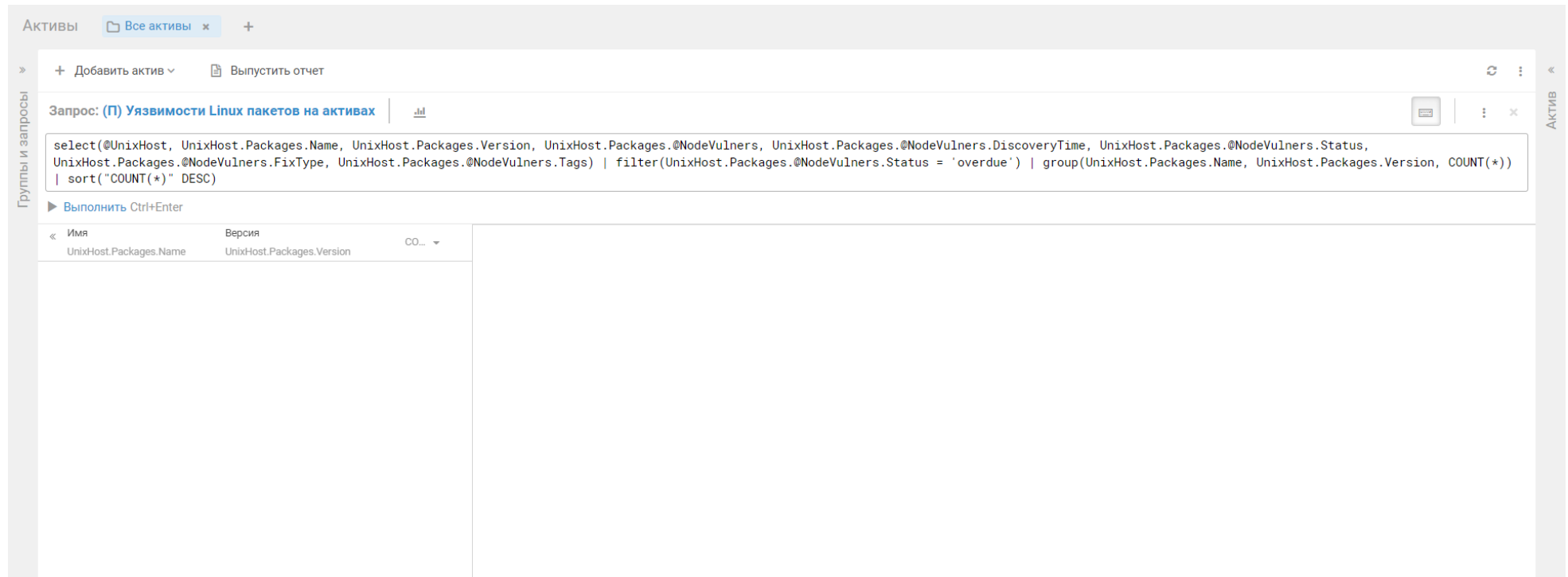
Виджет: «(П) Уязвимости Linux пакетов на активах»

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



The screenshot shows the MaxPatrol VM interface. At the top, there's a tab labeled "Активы" and a sub-tab "Все активы". Below that, there are buttons for "+ Добавить актив" and "Выпустить отчет". The main area is a query editor with the title "Запрос: (П) Уязвимости Linux пакетов на активах". The query text is:

```
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)
```

 Below the query editor, there's a button "Выполнить Ctrl+Enter". At the bottom, there's a table with columns "Имя" and "Версия". The table is currently empty, showing only the headers: "UnixHost.Packages.Name" and "UnixHost.Packages.Version".

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

Переходим в режим создания виджета нажатием соответствующей иконки:

The screenshot shows the MaxPatrol VM interface in the widget creation mode. The top bar includes 'Активы' and 'Все активы'. Below it, there are options for 'Экспорт' and 'Сохранить в библиотеку виджетов'. The main area displays a search query: '(П) Уязвимости Linux пакетов на активах'. Below the query, there are filters: '@UnixHost, UnixHost.Packages.Name, UnixHost.Packages.@NodeVulners.Status...'. The visualization settings panel on the left shows 'COUNT(*)' selected for the visualization type. The main area displays a 'Нет данных' (No data) message.

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 ИТ по данному типу уязвимостей отсутствуют

The screenshot shows the MaxPatrol VM interface. At the top, there's a tab labeled 'Активы' and a sub-tab 'Все активы'. Below that, there are buttons for '+ Добавить актив' and 'Выпустить отчет'. The main area is a query editor with the title 'Запрос: (П) Уязвимости Linux пакетов на активах (по хостам)'. The query text is: `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)`. Below the query editor, there's a button 'Выполнить Ctrl+Enter'. At the bottom, there's a table with columns: 'Узел', 'Имя', 'Версия', and 'Ко...'. The table is currently empty, showing only the header row with the first cell containing '@UnixHost'.

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

Переходим в режим создания виджета нажатием соответствующей иконки:

The screenshot shows the MaxPatrol VM interface in the widget creation mode. The top bar includes 'Активы' and 'Все активы'. The main area displays a search query: '(П) Уязвимости Linux пакетов на активах (по хостам)'. Below the search bar, there are filters and sorting options. The left sidebar shows the 'Отображение данных' (Data Display) settings, with 'Таблица' (Table) selected. A 'Нет данных' (No data) message is displayed in the main area.

Сохраняем получившийся виджет в библиотеку виджетов нажатием соответствующей кнопки.

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

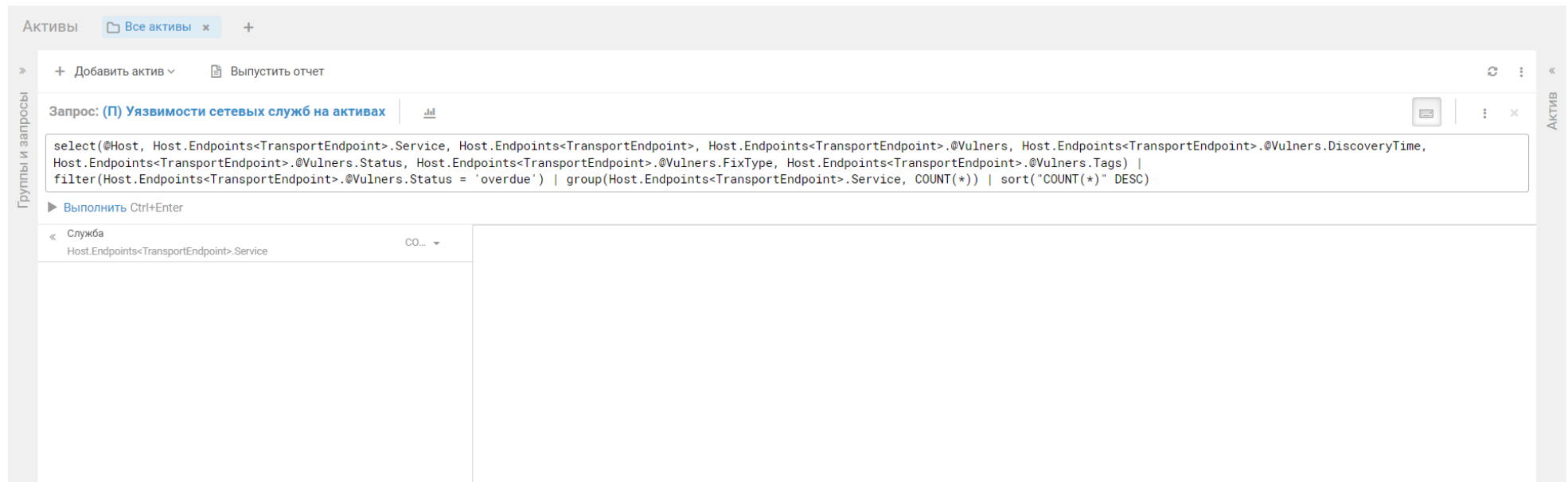
Виджет: «(П) Уязвимости сетевых служб на активах»

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 ИТ по данному типу уязвимостей отсутствуют



The screenshot shows the MaxPatrol VM interface. At the top, there's a navigation bar with 'Активы' and 'Все активы'. Below it, there's a search bar with the query '(П) Уязвимости сетевых служб на активах'. The query editor contains the following query:

```
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)
```

Below the query editor, there's a 'Выполнить Ctrl+Enter' button. The table view below shows a single column 'Служба' with a value 'Host.Endpoints<TransportEndpoint>.Service'.

Переходим в режим создания виджета нажатием соответствующей иконки:

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

Активы Все активы x +

Экспорт Сохранить в библиотеку виджетов

Запрос: (П) Уязвимости сетевых служб на активах

@Host, Host.Endpoints<TransportEndpoi... Host.Endpoints<TransportEndpoint>.@Vu... Host.Endpoints<TransportEndpoint>.Ser... COUNT(*) DESC

Выполнить

Группы и запросы

Показать: COUNT(*)

Отображение данных

- Таблица
- Столбчатая диаграмма
- График
- Круговая диаграмма

Гистограмма с накоплением

Логарифмическая шкала

Легенда

Только цвет, без подписей

Расположение

- Сверху
- Справа

Подписи данных на диаграмме

Нет данных

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)»

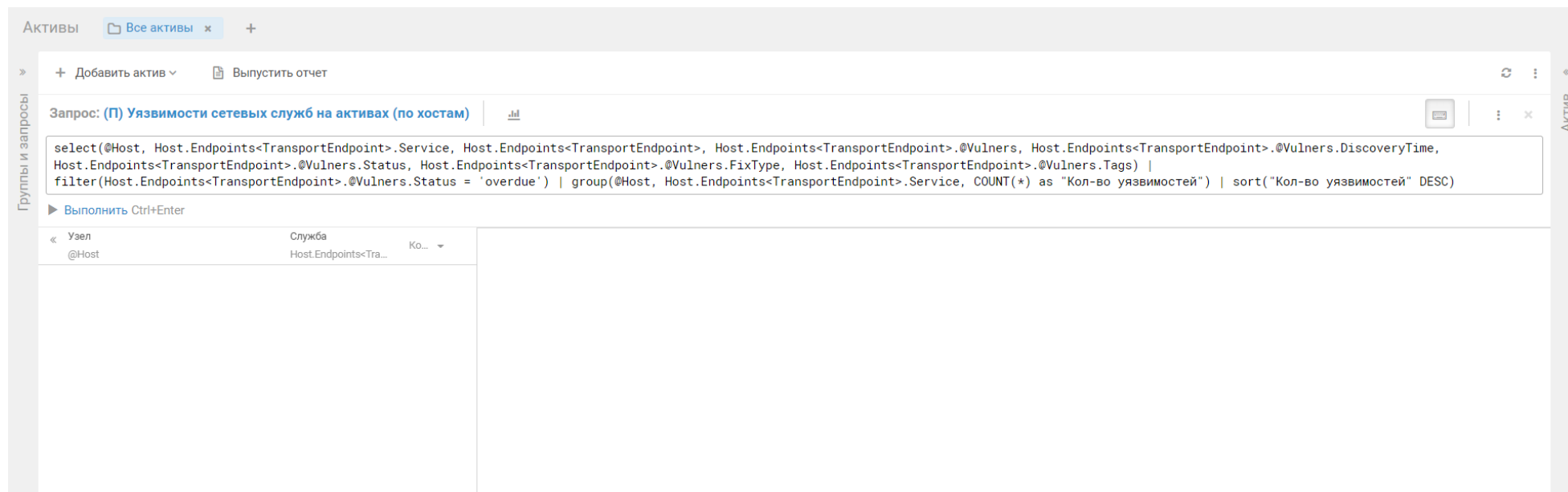
Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

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 ИТ по данному типу уязвимостей отсутствуют



The screenshot shows the MaxPatrol VM interface. At the top, there's a tab labeled 'Активы' and a sub-tab 'Все активы'. Below this, there's a search bar with the query: 'Запрос: (П) Уязвимости сетевых служб на активах (по хостам)'. The query text is: `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)`. Below the query editor, there's a button 'Выполнить Ctrl+Enter'. At the bottom, there's a table with columns 'Узел', 'Служба', and 'Ко...'. The table contains one row with the value '@Host' under 'Узел' and 'Host.Endpoints<Tra...' under 'Служба'.

Переходим в режим создания виджета нажатием соответствующей иконки:

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

Активы Все активы x +

Экспорт Сохранить в библиотеку виджетов

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

Поиск: @Host, Host.Endpoints<TransportEndpoi... Host.Endpoints<TransportEndpoint>.@Vu... @Host, Host.Endpoints<TransportEndpoi... Кол-во уязвимостей DESC Выполнить

Показать: Кол-во уязвимостей

Отображение данных

- Таблица
- Столбчатая диаграмма
- График
- Круговая диаграмма

Показать сумму по столбцу

Показать сумму по строке

Перевернуть таблицу

Нет данных

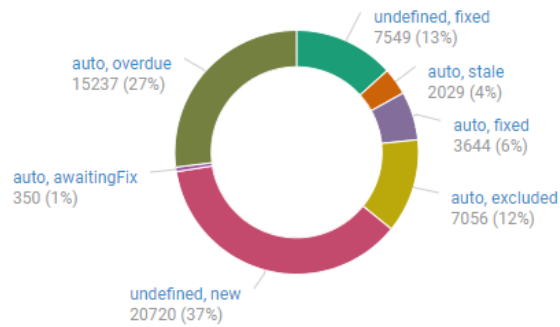
Сохраняем получившийся виджет в библиотеку виджетов нажатием соответствующей кнопки.

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

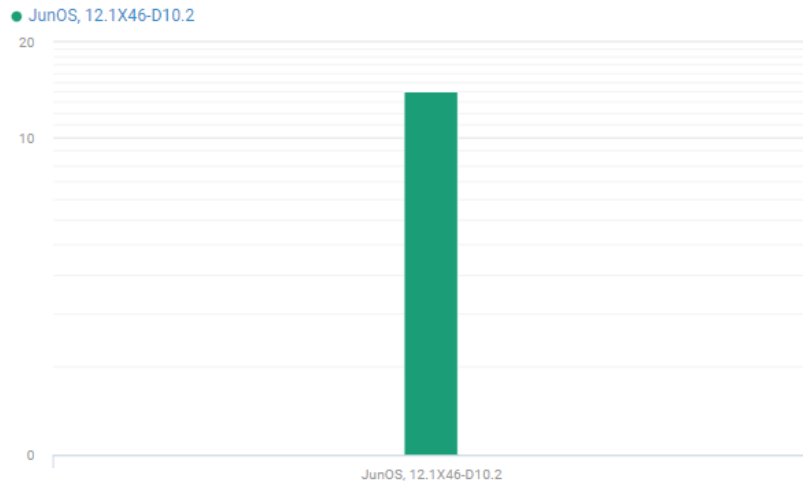
7. Отчёт о «слепых зонах» в процессе патч-менеджмента ИТ

(Н) Статистика по статусам покрытия уязвимостей

● undefined, fixed ● auto, stale ● auto, fixed ● auto, excluded ● undefined, new
● auto, awaitingFix ● auto, overdue



(Н) Уязвимости ОС на активах



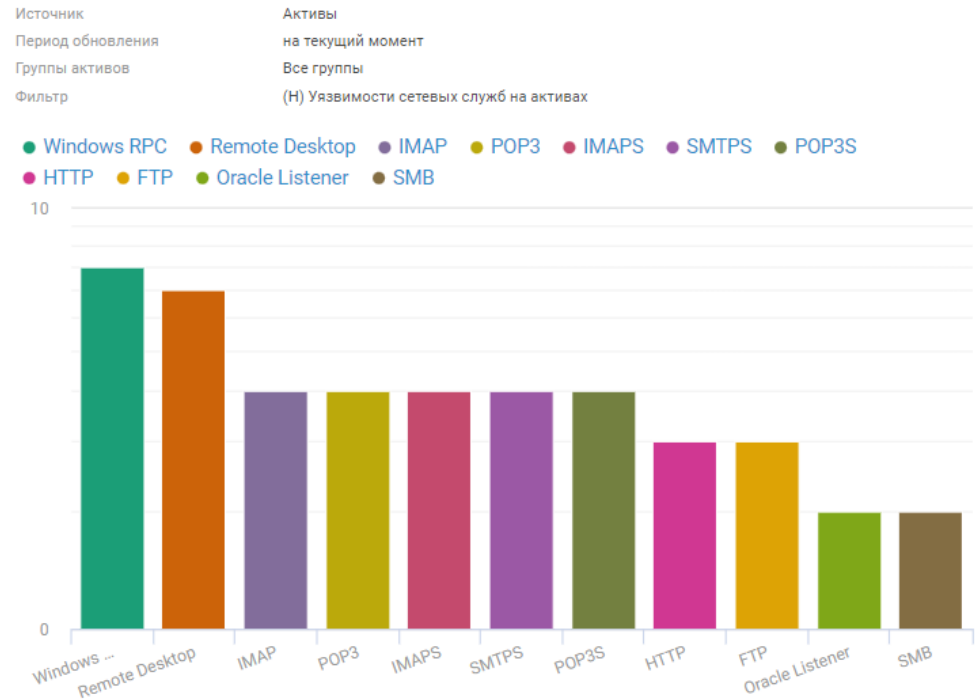
(Н) Уязвимости ПО на активах

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

(Н) 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...

(Н) Уязвимости сетевых служб на активах



Виджет: «(Н) 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(*))
```

The screenshot displays the MaxPatrol VM interface. At the top, there's a navigation bar with 'Активы' and 'Все активы'. Below it, a search bar contains the query: `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(*))`. Below the query editor, a table shows the results of the query. The table has columns for 'Устранение', 'Статус уязвимости', 'COUNT', 'Узел', 'Уязвимость', 'Дата и время обнаруж...', 'Статус уязвимости', 'Устранение', 'Важная', and 'Метки уязвимости'. The first row is highlighted in blue and shows 'Нет политики' with a status of 'Устранена' and a count of 7549. Other rows show various vulnerability types like 'Плановое', 'Удаленное выполнение кода', and 'Уязвимость CVE-2017-12173' with their respective counts and statuses.

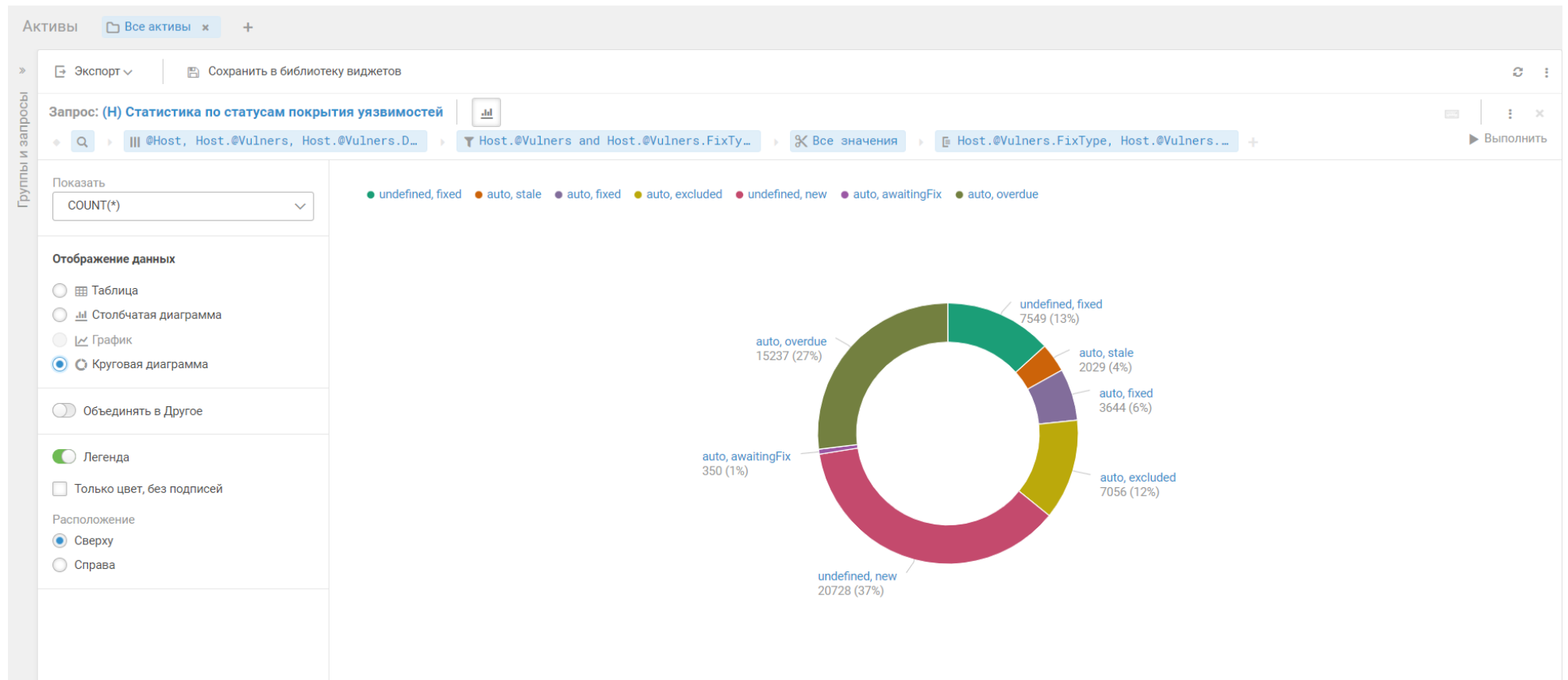
Устранение	Статус уязвимости	COUNT	Узел	Уязвимость	Дата и время обнаруж...	Статус уязвимости	Устранение	Важная	Метки уязвимости
Host.@Vulners.FixType	Host.@Vulners.Status		@Host	Host.@Vulners	Host.@Vulners.DiscoveryTime	Host.@Vulners.Status	Host.@Vulners.FixType	Host.@Vulners.IsDanger	Host.@Vulners.Tags
Нет политики	Устранена	7549	srv6.company.com (192.168.0.11)	Удаленное выполнение кода	20 февраля, 19:18	Устранена	Нет политики	False	null
Плановое	Требуется проверка	2029	srv6.company.com (192.168.0.11)	Удаленное выполнение кода	20 февраля, 19:18	Устранена	Нет политики	False	null
Плановое	Устранена	3644	srv12.company.com (192.168.0.17)	Уязвимость CVE-2017-12173	20 февраля, 19:18	Устранена	Нет политики	False	null
Плановое	Исключена	7056	srv12.company.com (192.168.0.17)	Уязвимость CVE-2012-2145	20 февраля, 19:18	Устранена	Нет политики	False	null
Нет политики	Новая	20728	srv12.company.com (192.168.0.17)	Уязвимость CVE-2010-5325	20 февраля, 19:18	Устранена	Нет политики	False	null
Плановое	Исправляется	350	srv12.company.com (192.168.0.17)	Уязвимость CVE-2015-8560	20 февраля, 19:18	Устранена	Нет политики	False	null
Плановое	Просрочено	15237	srv12.company.com (192.168.0.17)	Уязвимость CVE-2015-8327	20 февраля, 19:18	Устранена	Нет политики	False	null
			srv12.company.com (192.168.0.17)	Уязвимость CVE-2011-2964	20 февраля, 19:18	Устранена	Нет политики	False	null
			srv12.company.com (192.168.0.17)	Уязвимость CVE-2012-2677	20 февраля, 19:18	Устранена	Нет политики	False	null
			srv12.company.com (192.168.0.17)	Уязвимость CVE-2014-0062	20 февраля, 19:18	Устранена	Нет политики	False	null

Всего 7 группировок, выбрана 1

Всего 7549 записей, выбрана 1 запись (1 актив, 1 уязвимость)

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

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: «(Н) Уязвимости ОС на активах»

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

Вставляем и выполняем следующий запрос:

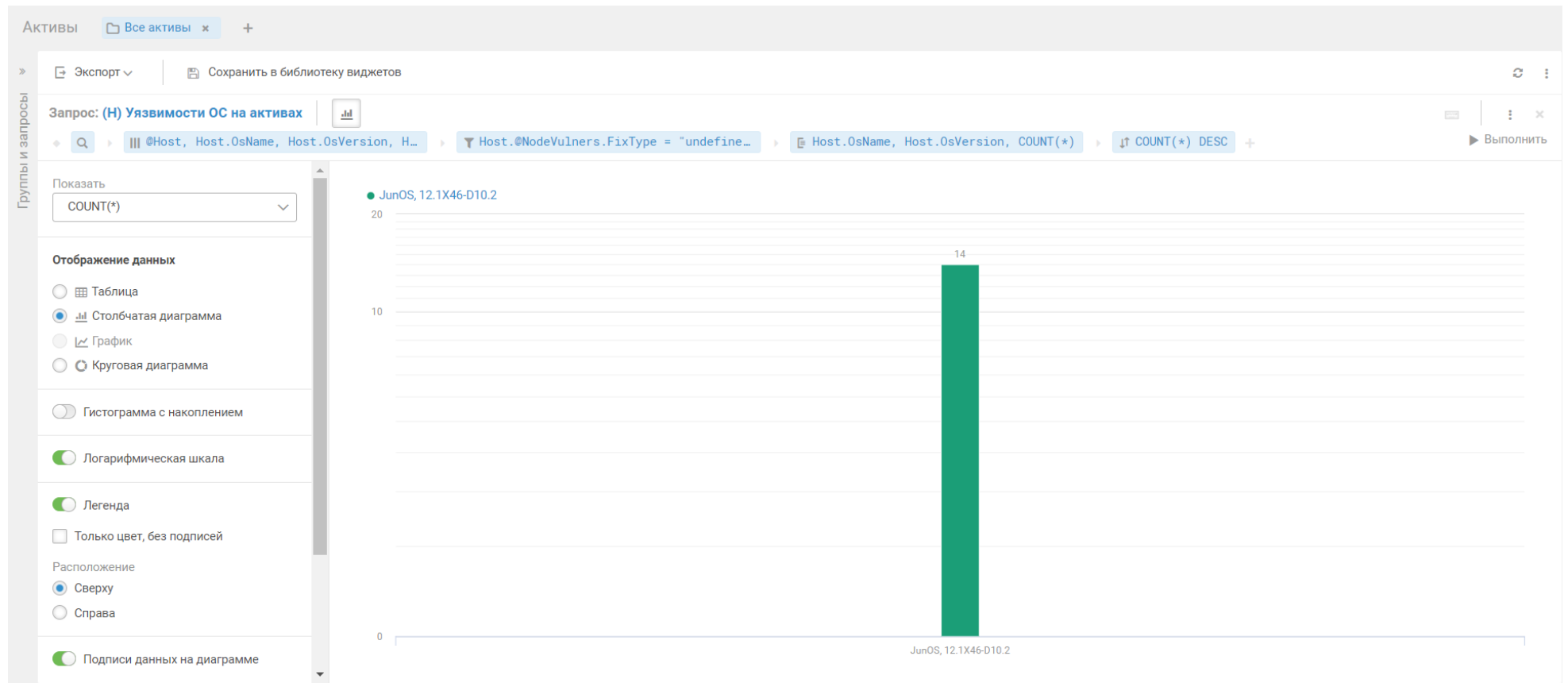
```
select(@Host, Host.OsName, Host.OsVersion, Host.@NodeVulners, Host.@NodeVulners.DiscoveryTime, Host.@NodeVulners.Status, Host.@NodeVulners.FixType, Host.@NodeVulners.Tags) | filter(Host.@NodeVulners.FixType = "undefined" and Host.@NodeVulners.Status = "new") | group(Host.OsName, Host.OsVersion, COUNT(*))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

The screenshot shows the MaxPatrol VM interface with a query executed. The query filters for new vulnerabilities with a fix type of 'undefined' and groups them by OS name and version. The results table shows 14 records for JunOS 12.1X46-D10.2, with various vulnerabilities listed.

Операционная система	Версия операцио...	COUNT(*)	Узел	Операционная сист...	Версия оп...	Уязвимость	Дата и время обнару...	Статус уязвимости	Устранение	Метки уязвимости
Host.OsName	Host.OsVersion		@Host	Host.OsName	Host.OsVe...	Host.@NodeVulners	Host.@NodeVulners...	Host.@NodeVulners...	Host.@NodeVulners...	Host.@NodeVulners...
JunOS	12.1X46-D10.2	14	router3.company.com (192.168.0...	JunOS	12.1X46-D...	Перехват сессии	20 февраля, 19:29	Новая	Нет политики	null
			router3.company.com (192.168.0...	JunOS	12.1X46-D...	Отказ в обслуживании	20 февраля, 19:29	Новая	Нет политики	null
			router3.company.com (192.168.0...	JunOS	12.1X46-D...	Разглашение информации	20 февраля, 19:29	Новая	Нет политики	null
			router3.company.com (192.168.0...	JunOS	12.1X46-D...	Отказ в обслуживании	20 февраля, 19:29	Новая	Нет политики	null
			router3.company.com (192.168.0...	JunOS	12.1X46-D...	Недостаточно быстрое запол...	20 февраля, 19:29	Новая	Нет политики	null
			router3.company.com (192.168.0...	JunOS	12.1X46-D...	Состояние гонки	20 февраля, 19:29	Новая	Нет политики	null
			router3.company.com (192.168.0...	JunOS	12.1X46-D...	Отказ в обслуживании	20 февраля, 19:29	Новая	Нет политики	null
			router3.company.com (192.168.0...	JunOS	12.1X46-D...	Отказ в обслуживании	20 февраля, 19:29	Новая	Нет политики	null
			router3.company.com (192.168.0...	JunOS	12.1X46-D...	Отказ в обслуживании	20 февраля, 19:29	Новая	Нет политики	null
			router3.company.com (192.168.0...	JunOS	12.1X46-D...	Отказ в обслуживании	20 февраля, 19:29	Новая	Нет политики	null
			router3.company.com (192.168.0...	JunOS	12.1X46-D...	Отказ в обслуживании	20 февраля, 19:29	Новая	Нет политики	null
			router3.company.com (192.168.0...	JunOS	12.1X46-D...	Состояние гонки	20 февраля, 19:29	Новая	Нет политики	null

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

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.

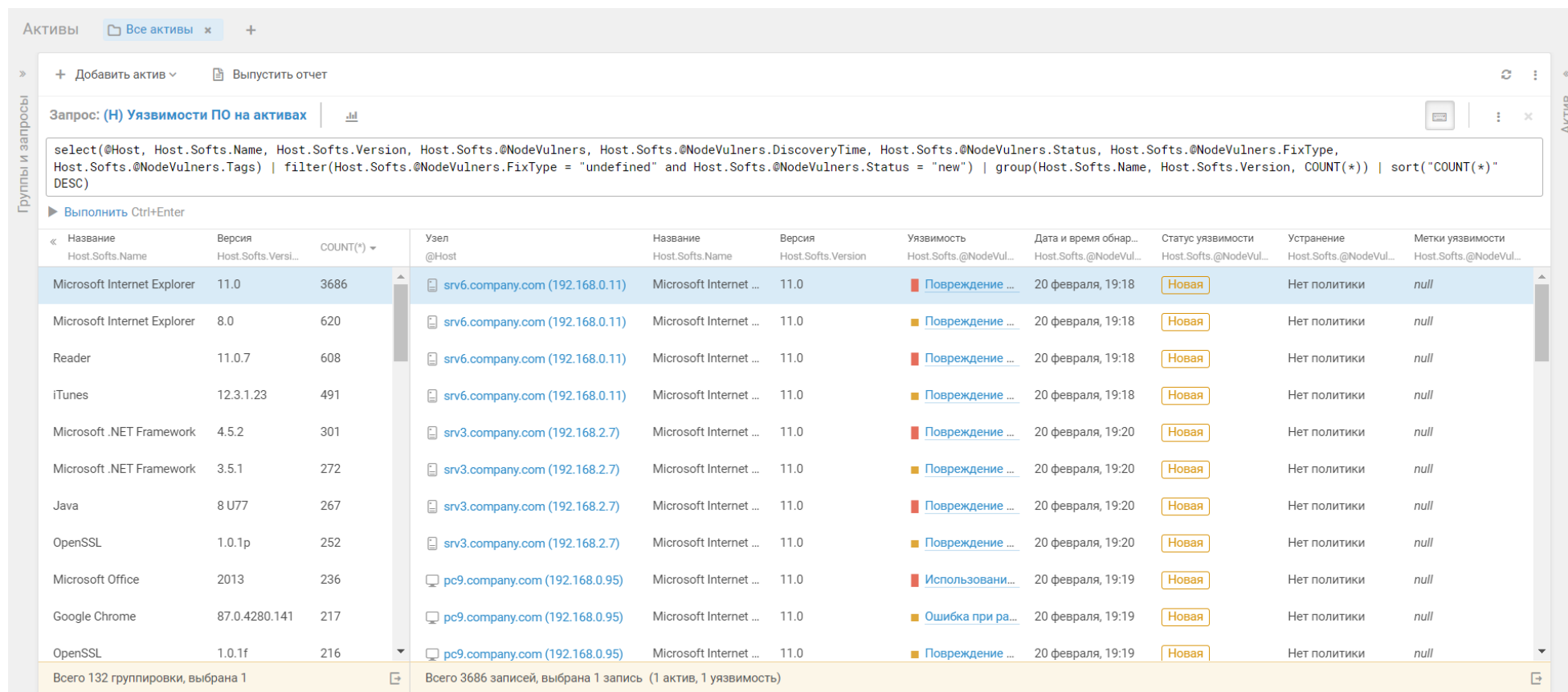
На вкладке «Система» -> «Отчёты» выбираем созданный ранее отчёт без шаблона и добавляем виджет.

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)
```

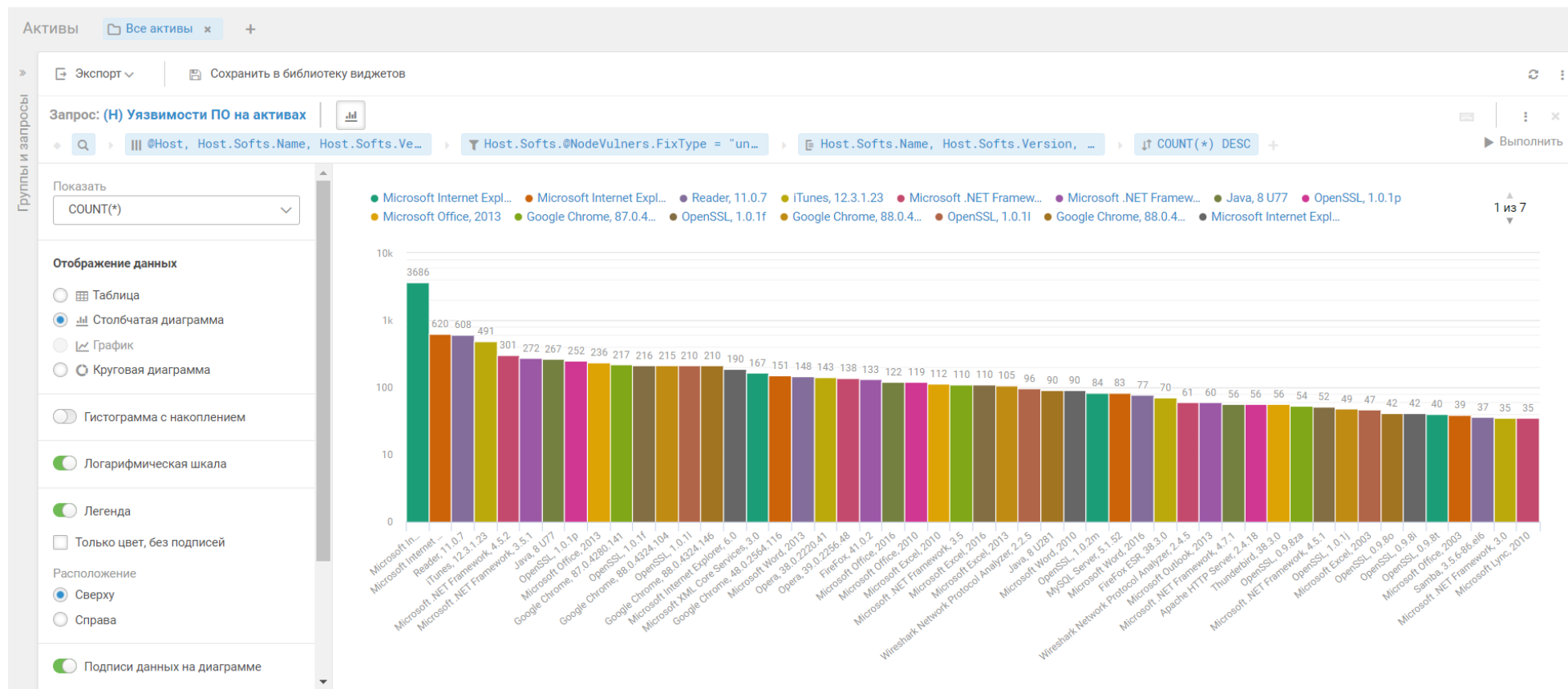


The screenshot displays the MaxPatrol VM interface. At the top, there's a navigation bar with 'Активы' and 'Все активы'. Below it, a search bar contains the query: '(Н) Уязвимости ПО на активах'. The query editor shows the full SQL query used for filtering and grouping. Below the query editor, a table lists the results of the query. The table has columns for software name, version, count, host, vulnerability name, version, status, discovery time, and fix type. The first row is highlighted, showing 'Microsoft Internet Explorer 11.0' with a count of 3686. The status is 'Новая' (New) and the fix type is 'Нет политики' (No policy).

Название	Версия	COUNT(*)	Узел	Название	Версия	Уязвимость	Дата и время обнаружения	Статус уязвимости	Устранение	Метки уязвимости
Host.Softs.Name	Host.Softs.Version		@Host	Host.Softs.Name	Host.Softs.Version	Host.Softs.@NodeVulners	Host.Softs.@NodeVulners	Host.Softs.@NodeVulners	Host.Softs.@NodeVulners	Host.Softs.@NodeVulners
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

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

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.

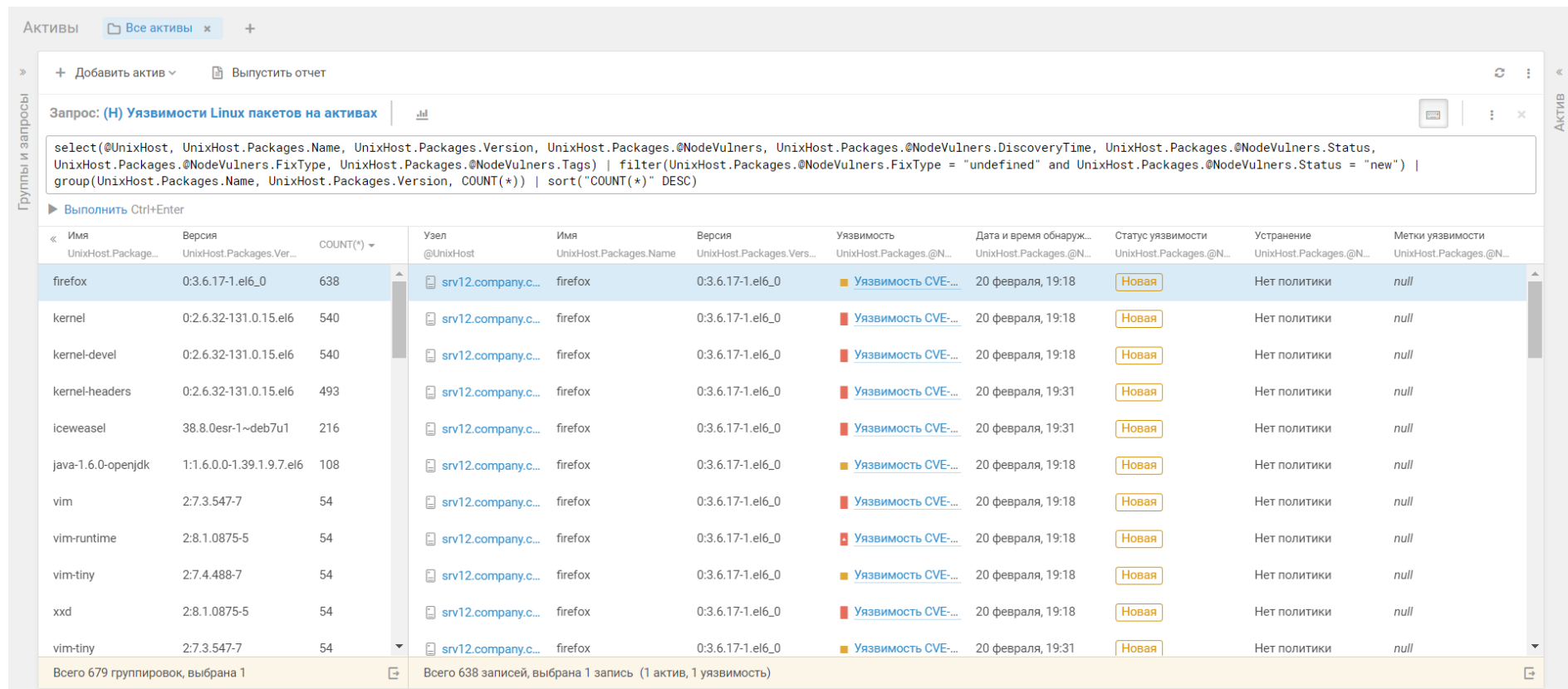
Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

Виджет: «(Н) 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)
```



The screenshot shows the MaxPatrol VM interface. At the top, there's a header with 'Активы' and 'Все активы'. Below it, a search bar contains the query: «(Н) Уязвимости Linux пакетов на активах». The query is pasted into a text area and executed. The results are displayed in a table with columns: Имя, Версия, COUNT(*), Узел, Имя, Версия, Уязвимость, Дата и время обнаруж..., Статус уязвимости, Устранение, and Метки уязвимости. The table lists various packages like firefox, kernel, and vim, along with their versions and the number of vulnerabilities found. The status of each vulnerability is marked as 'Новая' (New).

Имя	Версия	COUNT(*)	Узел	Имя	Версия	Уязвимость	Дата и время обнаруж...	Статус уязвимости	Устранение	Метки уязвимости
firefox	0:3.6.17-1.el6_0	638	srv12.company.c...	firefox	0:3.6.17-1.el6_0	Уязвимость CVE...	20 февраля, 19:18	Новая	Нет политики	null
kernel	0:2.6.32-131.0.15.el6	540	srv12.company.c...	firefox	0:3.6.17-1.el6_0	Уязвимость CVE...	20 февраля, 19:18	Новая	Нет политики	null
kernel-devel	0:2.6.32-131.0.15.el6	540	srv12.company.c...	firefox	0:3.6.17-1.el6_0	Уязвимость CVE...	20 февраля, 19:18	Новая	Нет политики	null
kernel-headers	0:2.6.32-131.0.15.el6	493	srv12.company.c...	firefox	0:3.6.17-1.el6_0	Уязвимость CVE...	20 февраля, 19:31	Новая	Нет политики	null
iceweasel	38.8.0esr-1~deb7u1	216	srv12.company.c...	firefox	0:3.6.17-1.el6_0	Уязвимость CVE...	20 февраля, 19:31	Новая	Нет политики	null
java-1.6.0-openjdk	1:1.6.0.0-1.39.1.9.7.el6	108	srv12.company.c...	firefox	0:3.6.17-1.el6_0	Уязвимость CVE...	20 февраля, 19:18	Новая	Нет политики	null
vim	2:7.3.547-7	54	srv12.company.c...	firefox	0:3.6.17-1.el6_0	Уязвимость CVE...	20 февраля, 19:18	Новая	Нет политики	null
vim-runtime	2:8.1.0875-5	54	srv12.company.c...	firefox	0:3.6.17-1.el6_0	Уязвимость CVE...	20 февраля, 19:18	Новая	Нет политики	null
vim-tiny	2:7.4.488-7	54	srv12.company.c...	firefox	0:3.6.17-1.el6_0	Уязвимость CVE...	20 февраля, 19:18	Новая	Нет политики	null
xxd	2:8.1.0875-5	54	srv12.company.c...	firefox	0:3.6.17-1.el6_0	Уязвимость CVE...	20 февраля, 19:18	Новая	Нет политики	null
vim-tiny	2:7.3.547-7	54	srv12.company.c...	firefox	0:3.6.17-1.el6_0	Уязвимость CVE...	20 февраля, 19:31	Новая	Нет политики	null

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

Виджет: «(Н) 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)
```

The screenshot displays the MaxPatrol VM interface. At the top, there's a search bar with the query: «(Н) Уязвимости сетевых служб на активах». Below the query editor, a table lists the results of the query. The table has columns for Service, COUNT(*), Узел, Служба, Конечные точки, Уязвимость, Дата и время обнаруж..., Статус уязвимости, Устранение, and Метки уязвимости. The first row is highlighted in blue and shows Windows RPC with a count of 7, located at 192.168.0.77, with a vulnerability of 'Удаленное выбо...' discovered on 20 февраля, 19:17, with a status of 'Новая' and no mitigation.

Служба	COUNT(*)	Узел	Служба	Конечные точки	Уязвимость	Дата и время обнаруж...	Статус уязвимости	Устранение	Метки уязвимости
Windows RPC	7	192.168.0.77	Windows RPC	49664/tcp	Удаленное выбо...	20 февраля, 19:17	Новая	Нет политики	null
Remote Desktop	6	192.168.0.77	Windows RPC	49665/tcp	Удаленное выбо...	20 февраля, 19:17	Новая	Нет политики	null
IMAP	3	192.168.0.77	Windows RPC	49666/tcp	Удаленное выбо...	20 февраля, 19:17	Новая	Нет политики	null
POP3	3	192.168.0.77	Windows RPC	49667/tcp	Удаленное выбо...	20 февраля, 19:17	Новая	Нет политики	null
IMAPS	3	192.168.0.77	Windows RPC	49668/tcp	Удаленное выбо...	20 февраля, 19:17	Новая	Нет политики	null
SMTPTS	3	192.168.0.77	Windows RPC	49673/tcp	Удаленное выбо...	20 февраля, 19:17	Новая	Нет политики	null
POP3S	3	192.168.0.77	Windows RPC	49675/tcp	Удаленное выбо...	20 февраля, 19:17	Новая	Нет политики	null
HTTP	2								
FTP	2								
Oracle Listener	1								

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

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 


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.com (192.168.0.245)	20 фев, 19:29
	Важная Устранение: Вручную juniper Juniper JUNOS 12.1X46-D10.2	

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

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

Отчеты MaxPatrol VM — ключ к эффективному процессу управления уязвимостями

» 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