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

Скрытые угрозы в MS Exchange: почему перебор пользователей — это больше, чем просто ошибка

Автор: xh4vm, команда пентеста CyberOK

Введение

Всем привет! На связи xh4vm из команды пентеста CyberOK. Ранее мы анонсировали обнаружение уязвимости перебора пользователей в модуле Autodiscover продукта Microsoft Exchange Server. Уязвимости присвоен идентификатор BDU:2024-08516 в БДУ ФСТЭК, а также установлена базовая оценка по метрике CVSS 3.0 — 7.5 баллов.

В данной статье мы рассмотрим технические детали уязвимости, обсудим причины, по которым она заслуживает внимания со стороны специалистов в области информационной безопасности и разберем методы минимизации риска.

Предыстория

В процессе аудита информационной безопасности часто возникает необходимость в актуальном списке пользователей организации. Этот список может быть использован для анализа рисков, связанных с фишингом, подбором паролей, утечками данных, а также для проверки других методов получения первоначального доступа.

Существует множество различных подходов для решения данной задачи. На одном из проектов нашу команду заинтересовал таргет в виде MS Exchange Server. Почему именно он? В большинстве случаев MS Exchange Server доступен внешнему злоумышленнику, а также глубоко интегрирован с Active Directory, что создает дополнительные векторы для атак.

Технические детали

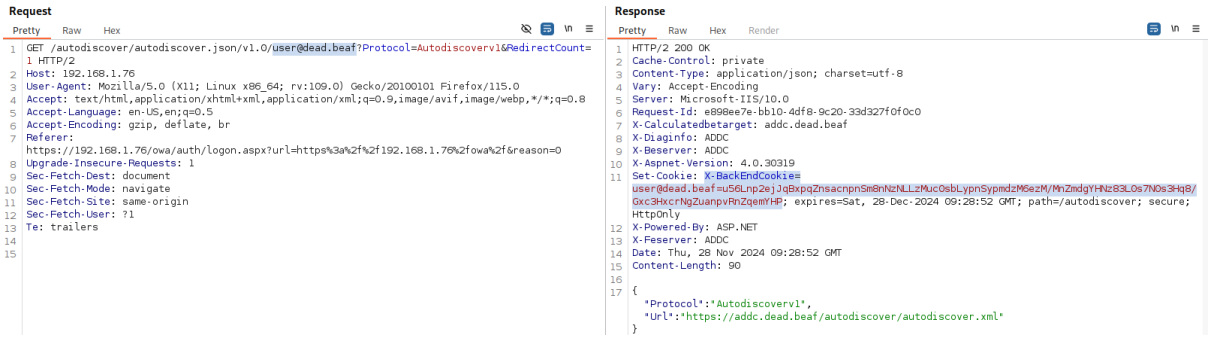
Уязвимость обнаружена в модуле Autodiscover и затрагивает все сборки продукта MS Exchange Server версии 2019 и 2016, включая патч от 12 ноября 2024 года. Уязвимость позволяет злоумышленнику определить наличие пользователя, основываясь на различиях в заголовках ответа веб-сервера. Если учетная запись зарегистрирована в базе данных MS Exchange Server, веб-сервер устанавливает значение для куки `X-BackEndCookie`, в противном случае это значение остается пустым.

Пример запроса для проверки наличия уязвимости:

```
GET /autodiscover/autodiscover.json/v1.0/<username>@<domain>?
Protocol=Autodiscoverv1&RedirectCount=1 HTTP/2
Host: <Host>
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
```

Пример ответа для существующего пользователя:

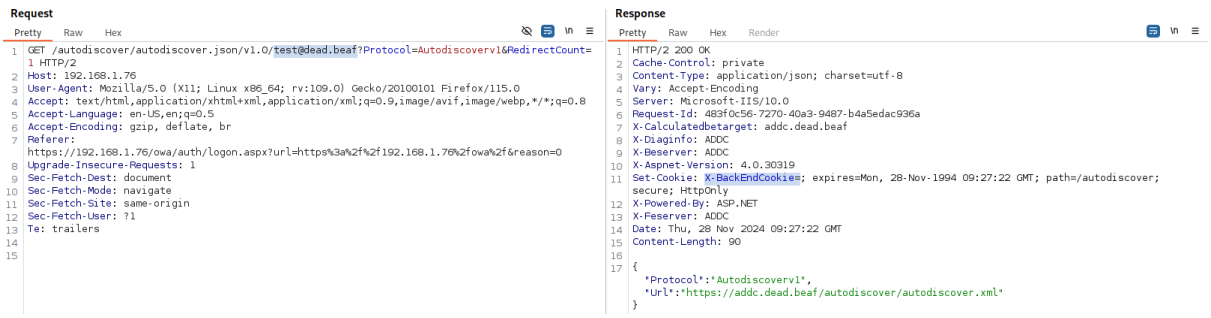
```
HTTP/2 200 OK
...
Set-Cookie: X-BackEndCookie=<username>@<domain>=<some value>; <other
cookie parameters>
...
```



Пример ответа для существующего пользователя. Автор: К. М. Епифанов, 2024.

Пример ответа для несуществующего пользователя:

```
HTTP/2 200 OK
...
Set-Cookie: X-BackEndCookie=; <other cookie parameters>
...
```



Пример ответа для несуществующего пользователя. Автор: К. М. Епифанов, 2024.

Для подтверждения концепции вы можете ознакомиться с кодом, размещенным в репозитории на GitHub.

Следует отметить, что уязвимость позволяет определить наличие только тех пользователей, которые зарегистрированы в базе данных MS Exchange Server. Это означает, что если пользователь существует в домене, но его почтовый аккаунт не создан, эксплуатация данной уязвимости не приведет к результатам. Кроме того, уязвимость не позволяет установить статус учетной записи:

- невозможно отличить доменную почтовую учетную запись от недоменной;
- заблокированные доменные учетные записи также могут отображаться в выборке, если не были удалены из MS Exchange Server.

Таким образом, злоумышленник может получить информацию о существующих пользователях, но с некоторыми ограничениями, что создает дополнительные сложности при анализе.

Векторы развития атаки

Как мы уже говорили, MS Exchange Server сильно интегрирован с Active Directory: каждый запрос на аутентификацию для доменного пользователя обрабатывается веб-сервером и перенаправляется к контроллеру домена. Некоторые из приведенных ниже векторов используют этот факт в своей основе.

1. Отказ в обслуживании

При наличии активной групповой политики блокировки учетных записей, определенное количество неуспешных попыток аутентификации может привести к нарушению рабочей деятельности пользователя.

Таким образом, обладая списком пользователей, злоумышленник может попытаться осуществить атаку типа «отказ в обслуживании» путем выполнения серии неуспешных попыток аутентификации, при этом важно равномерно распределить их количество среди всех учетных записей. Если же политика безопасности настроена более строго и включает блокировку административных учетных записей, последствия такой атаки могут оказаться более серьезными.

2. «Распыление» паролей

Чтобы избежать блокировки учетных записей, злоумышленник может прибегнуть к методу подбора пароля для различных пользователей. Этот подход оказывается достаточно эффективным на широком диапазоне учетных записей, поскольку, как показывает практика, многие пользователи могут использовать слабые или предсказуемые пароли.

3. Подбор пароля

Если учетная запись не подпадает под политику блокировки при неуспешных попытках аутентификации, злоумышленник может осуществить атаку по подбору аутентификационной информации, что значительно повышает его шансы на компрометацию этой учетной записи.

4. Фишинг

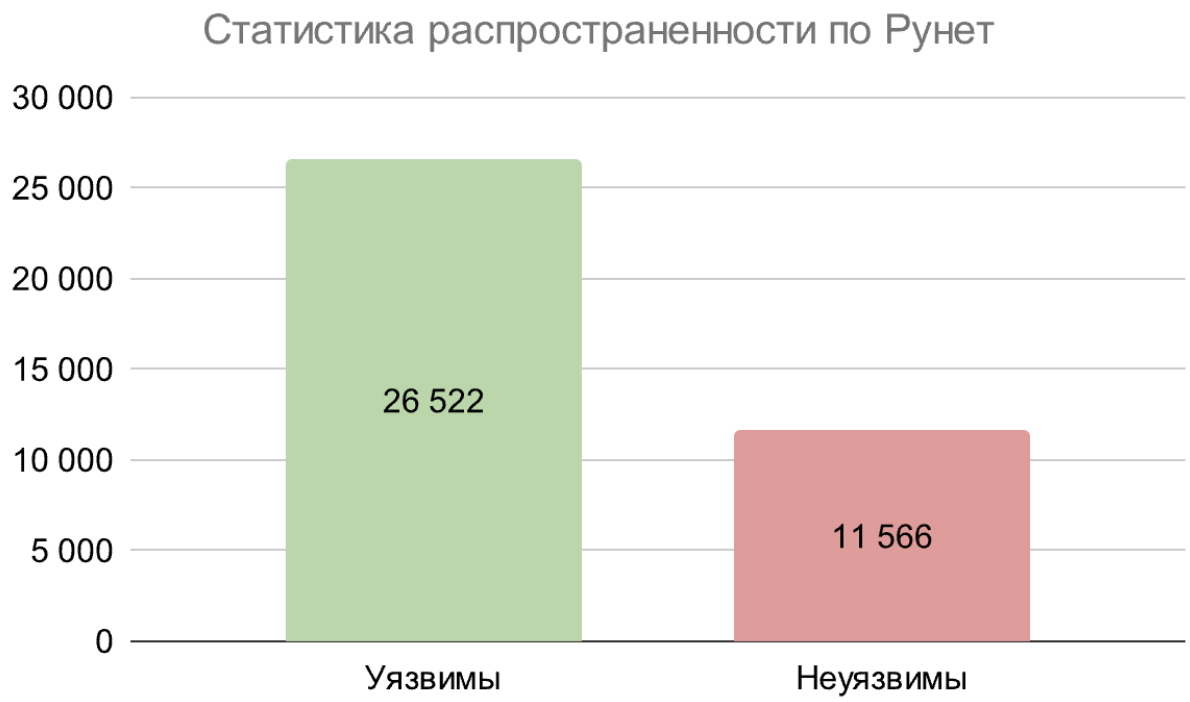
Наличие списка почтовых учетных записей значительно увеличивает риск фишинговых атак, так как злоумышленник может использовать эту информацию для проведения целевых кампаний, создавая правдоподобные сообщения и манипулируя эмоциями пользователей.

Также следует отметить, что организации часто сталкиваются с дополнительными уязвимостями в области информационной безопасности, такими как CVE-2024-49040, а также с ошибками конфигурации SMTP-сервера (как ни странно), которые могут позволить злоумышленнику отправить почтовое сообщение от имени произвольного пользователя без прохождения аутентификации. В таких случаях полученный список учетных записей может быть использован для выбора отправителя, что увеличит вероятность успеха фишинговой атаки, так как бдительность получателей будет снижена.

Результаты исследований

По данным аналитики **CyberOK СКИПА** за последние 3 месяца, в Рунете обнаружено около 38 тысяч инстансов MS Exchange Server, из которых, согласно публично доступной информации о версиях, более 31 тысячи потенциально подвержены уязвимости, что составляет более 83% от общего числа.

В ряде случаев предприняты меры по минимизации риска, в частности, ограничен анонимный доступ к виртуальному каталогу Autodiscover. Однако, несмотря на эти действия, доля потенциально уязвимых узлов по-прежнему составляет 70%.



Статистика распространенности по Рунет. Автор: К. М. Епифанов, 2024.

Минимизация риска

Не секрет, что Microsoft скептически относится к перебору пользователей в своих продуктах.

В статье «User Enumeration in Microsoft Products: An Incident Waiting to Happen?» компания Intruder уведомляет о возможных рисках, вызванных таким решением Microsoft. Согласно проведенному компанией исследованию, на момент 8 сентября 2023 года более 13 000 серверов «Skype для бизнеса» в сети Интернет уязвимы к перебору пользователей. При этом, один из методов подробно описан автором в личном блоге.

Исследователь сообщил об уязвимости 28 июня 2017 года, на что получил ответ — недостаток программного обеспечения не соответствует требованиям рассматриваемых проблем безопасности, поскольку не приводит к непосредственному доступу к ресурсу. В ноябре 2019 года описанная уязвимость была исправлена производителем, при этом регистрации и огласки не последовало.

Автор доклада «Track The Planet! Mapping IDs, Monitoring Presence In The Azure Ecosystem», представленного на конференции «DEF CON 31», призывает Microsoft пересмотреть отношение к перечислению пользователей. Исследователь утверждает, что данная проблема может не только привести к таким угрозам безопасности как фишинг и подбор аутентификационной информации, но и крайне нежелательна для сотрудников органов безопасности и политических организаций.

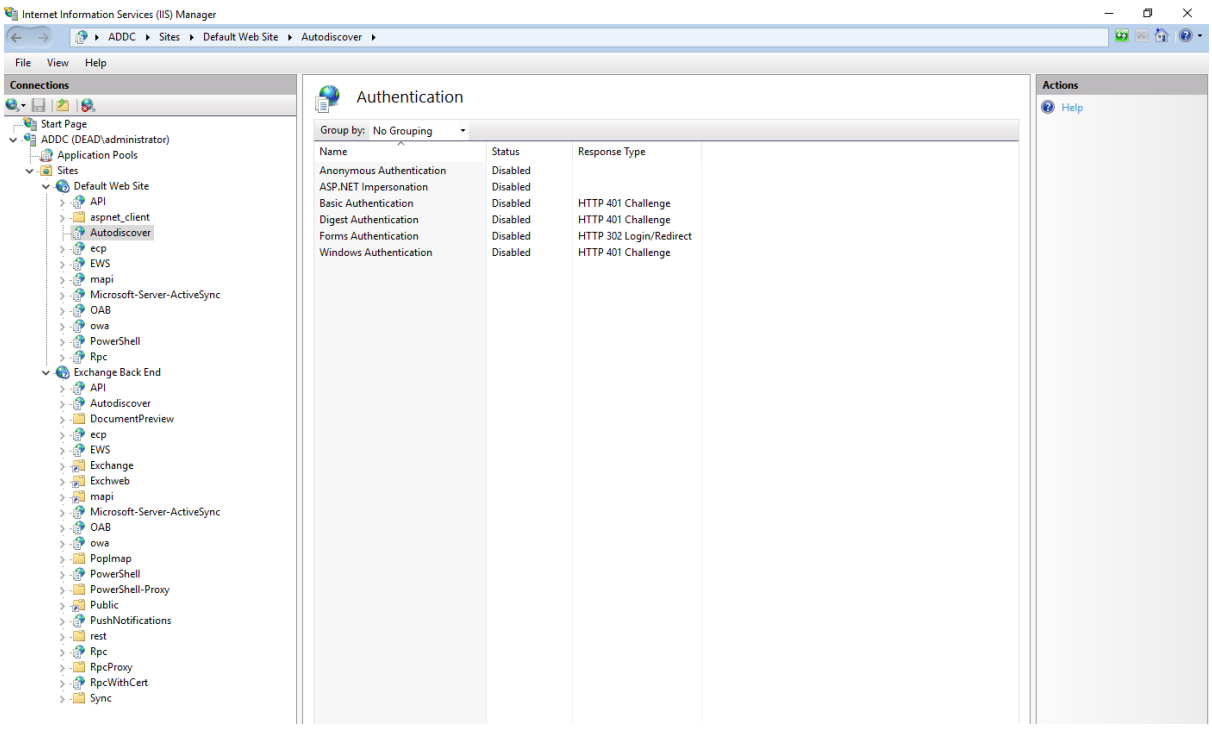
Исследователь обнаружил уязвимость перечисления пользователей в сервисе Microsoft OneDrive. Уведомление производителя не привело к исправлению недостатка. В то же время ответ вендора подчеркивает, что возможность перечисления пользователей во многих случаях является умышленной практикой. Исследователь воспользовался указанной особенностью продукта и запустил проект по перебору учетных записей. В результате, на момент выступления на конференции, им была собрана информация о 24 миллионах пользователей.

В результате нашего уведомления Microsoft, получен отказ в регистрации уязвимости и дальнейшем информировании пользователей. Приведенная причина: невысокий риск потенциальной атаки. На данный момент неизвестно, будет ли уязвимость исправлена.

Для минимизации риска необходимо внедрить ряд компенсирующих мер. Мы предлагаем рассмотреть несколько вариантов, которые помогут повысить уровень безопасности и защитить организацию от потенциальных угроз.

1. Аутентификация Autodiscover

Рекомендуем настроить аутентификацию для доступа к виртуальному каталогу Autodiscover. Для этого в конфигурации IIS-сервера следует перейти в настройки аутентификации для Autodiscover, выбрать подходящий тип и отключить анонимный доступ. После этого важно также настроить аутентификацию для всех клиентских приложений, чтобы гарантировать их корректную работу.

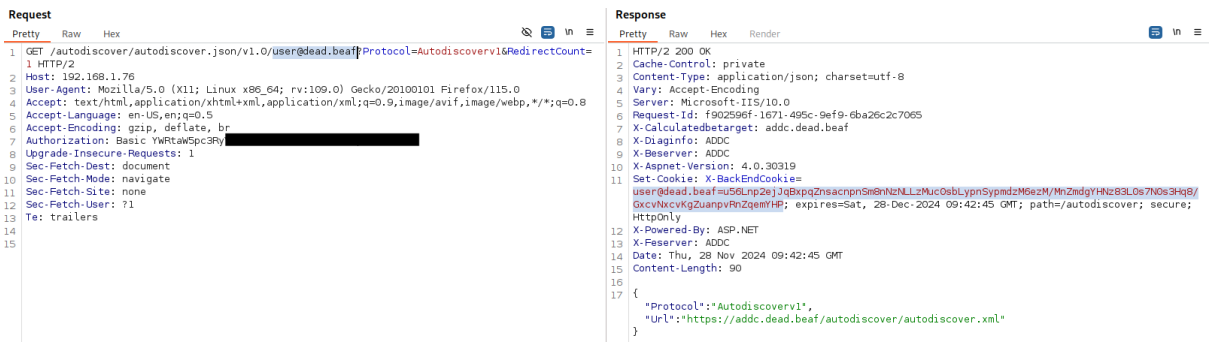


Конфигурация аутентификации Autodiscover. Автор: К. М. Епифанов, 2024.

Хотя данный вариант решения не устраняет уязвимость полностью, он создает дополнительные преграды в виде необходимости прохождения аутентификации. Если злоумышленник получит учетную запись для доступа к виртуальному каталогу, уязвимость вновь станет актуальной, но с одним небольшим отличием: при проверке несуществующей учетной записи cookie примет значение аутентифицированного пользователя.

Пример ответа для существующего пользователя с прохождением базовой аутентификации:

```
HTTP/2 200 OK
...
Set-Cookie: X-BackEndCookie=<username>@<domain>=<some value>; <other
cookie parameters>
...
```



Пример ответа для существующего пользователя с прохождением базовой аутентификации. Автор: К. М. Епифанов, 2024.

Пример ответа для несуществующего пользователя с прохождением базовой аутентификации:

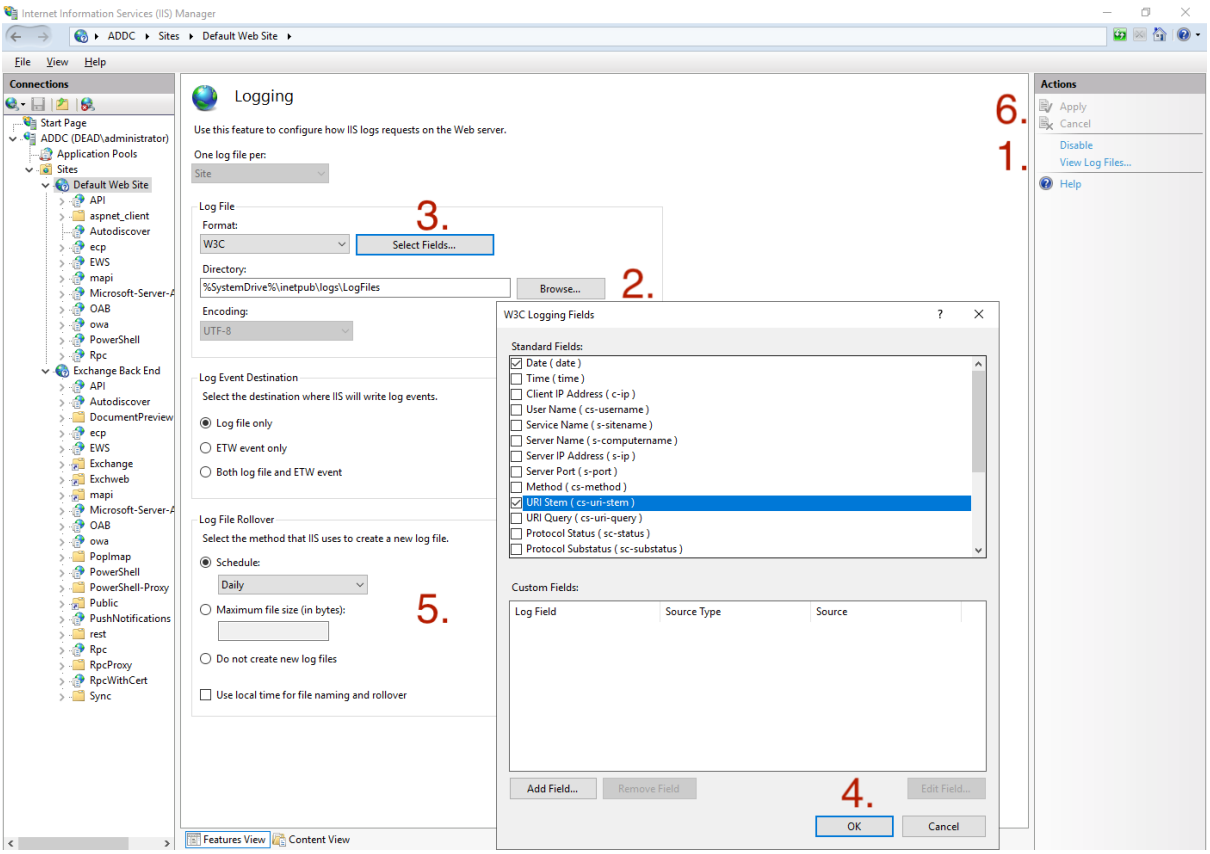
```
HTTP/2 200 OK
...
Set-Cookie: X-BackEndCookie=<SID>=<some value>; <other cookie parameters>
...
```

Пример ответа для несуществующего пользователя с прохождением базовой аутентификации. Автор: К. М. Епифанов, 2024.

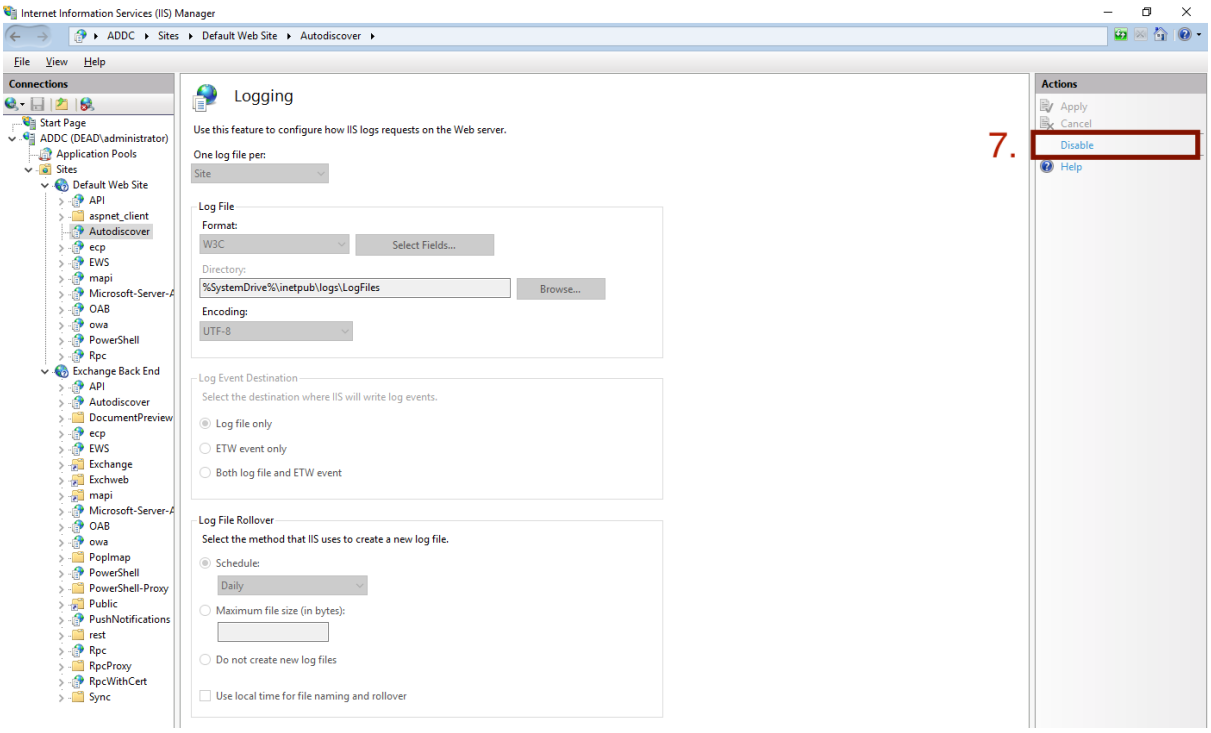
Мониторинг журналов IIS

Рекомендуем осуществить мониторинг журналов веб-сервера IIS. Для этого в конфигурации журналирования веб-сервера необходимо выполнить следующие шаги:

1. Убедиться, что функция журналирования включена.
2. Выбрать директорию, где будут храниться журналы веб-сервера. По умолчанию: %SystemDrive%\inetpub\logs\LogFiles.
3. Определить параметры, необходимые для анализа. Для эффективного обнаружения уязвимости активировать поле URI Stem, остальные параметры выбрать по необходимости.
4. Подтвердить выбор параметров записи журнала.
5. Установить принцип разбиения файлов.
6. Подтвердить все изменения.
7. Убедиться, что функция логирования активна для виртуального каталога Autodiscover. Для этого перейти в конфигурацию журналирования виртуального каталога Autodiscover.



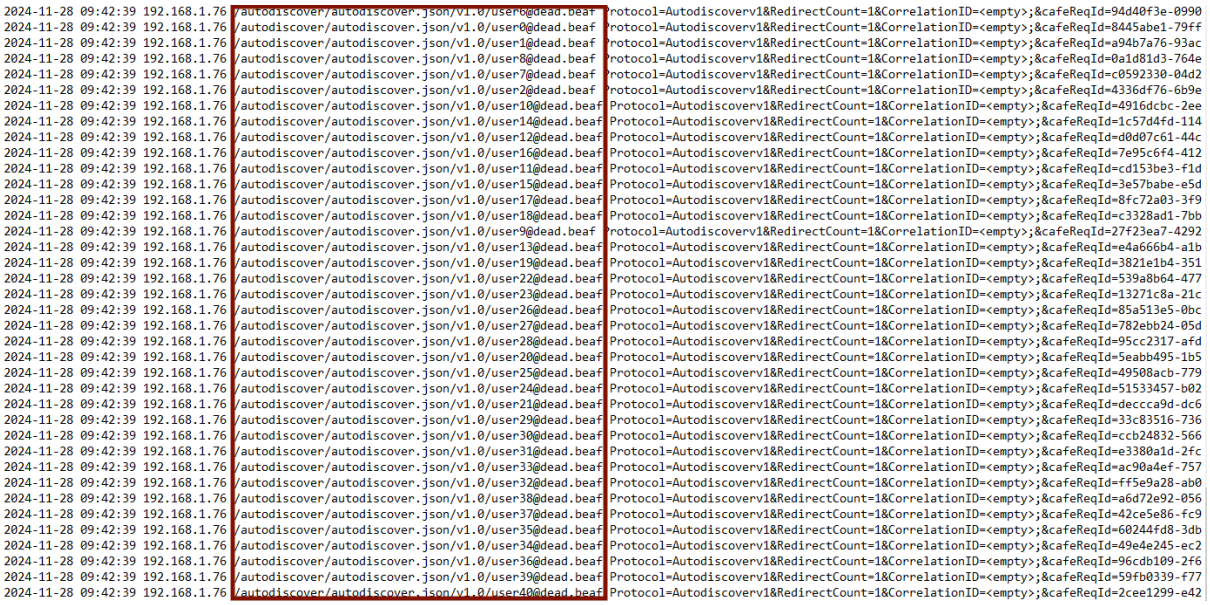
Шаг 1-6 настройки журналирования. Автор: К. М. Епифанов, 2024.



Шаг 7 настройки журналирования. Автор: К. М. Епифанов, 2024.

После выполнения всех шагов необходимо перезагрузить веб-сервер IIS, запустив команду `iisreset.exe`.

В процессе реализации атаки в журналах веб-сервера можно заметить аномально большое количество запросов для несуществующих учетных записей, что может служить индикатором эксплуатации уязвимости. Мониторинг позволит оперативно реагировать на подозрительную активность и принимать меры по укреплению безопасности системы.



Фрагмент журнала после проведения атаки по перебору пользователей. Автор: К. М. Епифанов, 2024.

Заключение

В данной статье мы рассмотрели уязвимость перебора пользователей в продукте Microsoft Exchange Server, проанализировали возможные векторы атак, которые могут возникнуть в результате эксплуатации и разобрали рекомендации по минимизации рисков.

Проблема остается актуальной, поэтому важно осознать потенциальные угрозы и принять соответствующие меры. Это поможет обеспечить безопасность корпоративной инфраструктуры.