УДК 004

И. А. Федореев[1]*

Улучшения ролевой модели в Azure DevOps

[1] Национальный исследовательский ядерный университет «МИФИ», г. Москва, Российская Федерация
* e-mail: maliferthebest1@gmail.com

Аннотация. В современных CI/CD системах одной из фундаментальных проблем эксплуатации является поддержание высокого уровня защищенности различных объектов программной инженерии. Безопасность проектов компании можно обеспечивать разными способами, например, встраиванием SAST, DAST и IAST анализаторов, использованием плагинов проверки на безопасность IaC у оркестратора. Но одним из самых простых и тривиальных методов поддержания уровня защищенности проектов, в первую очередь от атак инсайдера и человека посередине, является оптимально настроенная ролевая модель CI/CD системы, которая имеет четкую иерархию прав и привилегий. В рамках исследования возможности ролевой модели Azure DevOps был предложен ряд дополнительных мер по улучшению имеющейся структуры прав пользователей с точки зрения безопасности эксплуатации платформы.

Ключевые слова: CI/CD, Azure, DevSecOps, DevOps

I. A. Fedoreev[1]

Improvement to the Azure DevOps System Role Model

[1] National Research Nuclear University MEPhI, Moscow, Russian Federation
* e-mail: maliferthebest1@gmail.com

Abstract. In modern CI/CD systems, one of the fundamental problems of operation is maintaining a high level of security of various software engineering objects. The security of the company's projects can be ensured in different ways, for example, by embedding SAST, DAST and IAST analyzers, using IaC security check plugins in the orchestrator. But one of the simplest and most trivial methods of maintaining the level of project security, first of all, against insider and man-in-the-middle attacks, is an optimally configured role model of CI/CD system, which has a clear hierarchy of rights and privileges. As part of the Azure DevOps role model capability study, a number of additional measures have been proposed to improve the existing user rights structure in terms of secure platform operation.

Keywords: CI/CD, Azure, DevSecOps, DevOps

Введение

В связи с развитием технологий в сфере автоматизации процессов развертывания сборки ПО и дальнейшей доставки объектов программной инженерии на сервера эксплуатации, крупнейшие компании все чаще сталкиваются с новым видом атак злоумышленников на инфраструктуру. Согласно данным SailPoint [1], число атак на цепочку поставок с 2022 по 2023 год выросло на 115 %, что подчеркивает актуальность темы исследования и делает значимым разработку новых или модернизацию имеющихся комплексных методологий, направленных на повышение безопасности IaC (англ. Infrastructure as Code) внутри компании.

В качестве примера стоит привести одну из новых комплексных методологий в сфере ИБ – DevSecOps (англ. Development Security Operations), которая предлагает внедрение различных практик по кибербезопасности в уже устоявшееся направление DevOps. В данной области свои исследования проводят следующие ученые: Z. Pan, Donca I. C., Zhu L., Vadapalli S., Qumer Gill A., Серис А., Basynya E. [2–10].

Важным фактором, который будет значительно повышать уровень защищенности CI/CD (англ. Continuous Integration/ Continuous Delivery) процессов проектов в корпоративной среде, является ролевая модель CI/CD платформ [11], при помощи которых производится сборка и развертывание приложений. Технология позволяет наладить рабочий процесс разработки проекта в соответствии с обязанностями участников в развиваемом продукте и должностными обязанностями участников.

Одной из самых популярных CI/CD платформ на момент написания статьи является Azure DevOps [12], разработанная компанией Microsoft, отличительной особенностью которой является наличие необходимого функционала для покрытия всех этапов жизненного цикла проекта с точки зрения методологии DevSecOps и наиболее гибкой и проработанной ролевой модели по сравнению с конкурентами. Однако базовый набор ролей и их прав доступа, предлагаемых Microsoft, не соответствует современным реалиям в отношении разработки проектов, так как не учитывает наличие некоторых потенциальных участников проекта. Система предоставляет пользователям избыточные права доступа, наличие которых может привести к увеличению шанса внедрения НДВ (недокументированных возможностей) в разрабатываемый продукт, а также повышает возможности потенциального нарушителя, скомпрометировавшего данные учетной записи одного из участников проекта [13, 14].

В связи с вышеупомянутыми рисками предлагается пересмотреть перечень ролей и их прав чтобы привнести изменения в имеющуюся ролевую модель в Azure DevOps с целью повышения общей защищенности данной CI/CD системы.

В данной статье не будут рассматриваться группы пользователей и их права в отношении Azure Artifacts и Azure Testplan, поскольку данные сущности Azure DevOps не имеют прямого отношения к сборке и развертыванию проектов.

Принципы ролевой модели CI/CD системы

Целью данной работы является анализ имеющихся возможностей ролевой модели рассматриваемой CI/CD платформы и внесение предложений по изменению имеющегося функционала с точки зрения безопасности системы.

Для того чтобы построить систему управления правами в Azure DevOps, которая повысит общий уровень защищенности системы, следует воспользоваться несколькими моделями безопасности, применимыми для нашей системы.

1. Принцип нулевого доверия. Никто по умолчанию не обладает какими-либо правами в системе, и каждый пользователь перед получением новых прав или привилегий должен пройти обязательную процедуру аутентификации перед выдачей доступа.

2. Принцип минимальных привилегий. Если пользователю нужно получить дополнительные права, то ему будет выдан ровно тот необходимый перечень привилегий, который необходим ему для работы.

Прежде чем приступить к внесению предложений по улучшению ролевой модели, стоит ознакомиться с существующим списком стандартных ролей в системе Azure DevOps и их правами в ключевых компонентах системы, которые могут привести к созданию закладок в исходном коде и атак на цепочку поставок – Azure Repos и Azure pipelines [15, 16].

Исходя из существующего перечня ролей и привилегий, приведенных в табл. 1, можно сделать вывод, что в базовой ролевой модели отсутствуют какие-либо дополнительные роли для специалистов ИБ и проектных менеджеров, которые, согласно принципам DevSecOps [4], должны в обязательном порядке присутствовать. Поэтому предлагается изменить перечни привилегий для имеющихся ролей и привнести новые сущности, которые позволят соответствовать названному нами раннее принципу минимальных привилегий.

Таблица 1

Привилегии стандартных ролей в Azure Repos [12]

Разрешение	Читатель	Участник	Администратор сборки	Администратор проекта
Чтение	✓	✓	✓	✓
Участие	×	✓	✓	✓
Изменение репозиториев	×	×	×	✓
Изменение политик и разрешений	×	×	×	✓
Обход политик	×	×	×	×

Улучшения модели в Azure Repos

Перед описанием внедряемых инновационных практик стоит упомянуть о термине «коллекция» в понимании Azure DevOps. Так как данная система является комплексной и в ней может разрабатываться одновременно несколько проектов разными командами, то их можно объединять в группы, именуемые коллекциями. Данная особенность системы актуальна для исследования, так как позволяет выдавать роли, которые будут иметь более высокий приоритет над правами не только на уровне проектов, но и на уровне коллекций.

В качестве изменений предлагается сделать следующее.

1. Ввести на уровне коллекции роль «администратор безопасности», которая будет обладать всеми теми же правами с дополнительными правами по обходу политик и выдаче прав, помимо прав «администратор проекта», только на уровне коллекции, что позволит полностью делегировать обязанности по выдаче

прав участникам разработки проекта сотрудникам информационной безопасности и уменьшит риски избыточной выдачи прав. Права на обход политик и выдачу прав позволят своевременно среагировать на компрометации учетной записи в системе и лишить её всех привилегий.

2. Ввести на уровне проекта роль «менеджер проекта». Так как руководитель команды разработки в индустрии не принимает участия в создании исходного кода, а исполняет скорее административные и управленческие функции в проекте, то предоставляем ему только следующие роли в Azure Git:

– чтение;
– переименование репозитория;
– принудительная отправка;
– удаление репозитория;
– создание репозитория.

3. Ввести на уровне проекта роль «редактор политик». Изначально данная роль предполагает возможность внесения изменений в политику сборки приложения, в которой закладывается предварительная проверка проекта на уязвимости при помощи SAST и DAST решений, однако её можно временно выдавать участникам проекта для проведения тестирования различного функционала разрабатываемого ПО, который вызывает срабатывания политик безопасности. Также данная роль будет позволять изменять правило утверждения запросов на вытягивание в ветках и менять необходимое число рецензентов, необходимых для завершения запросов на вытягивание.

Данные роли касались исключительно Azure Git, и теперь можно перейти к правам доступа и ролям в Azure pipelines, при помощи которого осуществляется сборка и доставка приложений на сервера.

Аналогично случаю с Azure Repos стандартный набор ролей, приведенный в табл. 2 и предлагаемый Azure для агрегации доступа к конвейерам, является недостаточно гибким и глубоким для того, чтобы им можно было обходиться с поддержанием высокого уровня защищенности системы и принципа минимальных привилегий.

Таблица 2

Привилегии стандартных ролей в Azure Pipelines [12]

Разрешение	Читатель	Соавтор	Администратор сборки	Администратор проекта	Администратор выпуска
Просмотр конвейеров выпуска	✓	✓	✓	✓	✓
Определение сборок	×	✓	✓	✓	×
Определение выпусков	×	✓	×	✓	✓
Утверждение выпусков	×	✓	✓	✓	✓
Доступ к Azure Artifacts	×	✓	×	✓	✓
Создание очередей сборки	×	✓	×	×	×

Разрешение	Читатель	Соавтор	Администратор сборки	Администратор проекта	Администратор выпуска
Редактирование политик очередей сборки	×	×	✓	✓	×
Управление политиками хранения сборок	×	✓	✓	✓	×
Выдача разрешений на сборку	×	×	✓	✓	×
Управление разрешениями на выпуск	×	×	×	✓	✓
Редактирование групп задач	×	✓	✓	✓	✓
Управление разрешениями групп задач	×	×	✓	✓	✓
Просмотр пространства библиотеки	×	✓	✓	✓	✓
Использование и управление элементами библиотеки	✓	×	✓	✓	✓

Улучшения модели в Azure Pipelines

Следует отдельно отметить, что в современных методологиях разработки всегда предполагается тестирование проекта в отдельных тестовых средах перед тем, как опубликовать проект в продуктовой среде, поэтому изменения будут вводиться в том числе исходя из необходимости разделения ролей участников на выпуск ПО в релиз или тестовую среду.

На данном этапе будут предложены следующие изменения в правах доступа для стандартного набора ролей Azure DevOps и привнесения новых сущностей.

1. Поскольку основные задачи по сборке проекта в текущих реалиях популярных методологий разработки (например, Agile) выполняют не сами разработчики, а DevOps инженеры, то у группы пользователей «соавторы» необходимо убрать все привилегии, кроме привилегии «просмотр конвейеров выпуска».

2. У каждой роли в Azure DevOps кроме создателя платформы не должно быть привилегии «удалить сборку», так как данное право позволяет потенциальному злоумышленнику уничтожать улики после внедрения ВПО в исходный код конвейера (защита от атаки на цепочку поставок).

3. У ролей «администратор сборки» и «администратор проекта» не должно быть прав на изменение прав сборки приложения относительно других ролей и своей собственности. Это связано с тем, что Azure DevOps на уровне архитектуры имеет уязвимость, которая заключается в том, что пользователь может сам себе выдавать дополнительные привилегии в том случае, если отсутствует правило на более верхнем уровне, которое запрещает ему обладать этими правами.

4. Исходя из раннее упомянутого пункта о внедрении дополнительной роли «администратор безопасности», администратор будет обладать перечнем всех прав, которые приведены в таблице 2.

5. Исходя из раннее упомянутого пункта о внедрении дополнительной роли «менеджер проекта», пользователь с данным правом будет обладать только правом просматривать конвейеры сборки и выпуска приложений, так как он исполняет исключительно управленческую функцию.

Заключение

В результате рассмотрения ролевой модели Azure DevOps и выделения основных её недостатков был сформулирован и предложен ряд мер по её улучшению, не изменяя исходного кода продукта и основываясь только на существующем функционале. Были предложены изменения в имеющихся привилегиях для существующих ролей и добавлены новые сущности в виде отдельных групп и ролей. Введенные изменения позволят в определенной степени увеличить защищенность системы Azure DevOps от инсайдерских и middleware атак.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Supply chain attack // SailPoint. – URL: https://www.sailpoint.com/identity-library/supply-chain-attack (дата обращения: 22.04.2024).

2. Басыня, Е. А. Комплексная методология интеллектуально-адаптивного управления информационной инфраструктурой предприятия / Е. А. Басыня // Защита информации. Инсайд. – 2021. – № 5(101). – С. 16-25.

3. Басыня, Е. А. Метод идентификации киберпреступников, использующих инструменты сетевого анализа информационных систем с применением технологий анонимизации / Е. А. Басыня, В. Е. Хиценко, А. А. Рудковский // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2019. – Т. 22, No 2. – С. 45-51.

4. Басыня Е. А. Распределенная система сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия // Безопасность информационных технологий. – 2018. – Т. 25. – № 4. – С. 42-51.

5. Shahin, M., Babar, M.A. and Zhu, L., 2017. Continuous integration, delivery and deployment: a systematic review on approaches, tools, challenges and practices. IEEE access, 5, pp.3909-3943.

6. Z. Pan et al., "Ambush From All Sides: Understanding Security Threats in Open-Source Software CI/CD Pipelines," in IEEE Transactions on Dependable and Secure Computing, vol. 21, no. 1, pp. 403-418, Jan.-Feb. 2024, doi: 10.1109/TDSC.2023.3253572.

7. Donca I. C. et al. Method for continuous integration and deployment using a pipeline generator for agile software projects // Sensors. – 2022. – Т. 22. – №. 12. – С. 4637.

8. Vadapalli S. DevOps: continuous delivery, integration, and deployment with DevOps: dive into the core DevOps strategies. – Packt Publishing Ltd, 2018.

9. Qumer Gill A. et al. DevOps for information management systems // VINE Journal of Information and Knowledge Management Systems. – 2018. – Т. 48. – №. 1. – С. 122-139.

10. Серис А. et al. Implementation of a continuous integration and deployment pipeline for containerized applications in amazon web services using jenkins, ansible and kubernetes // 2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet). – IEEE, 2020. – С. 1-6.

11. Hsu T. H. C. Hands-On Security in DevOps: Ensure continuous security, deployment, and delivery with DevSecOps. – Packt Publishing Ltd, 2018.

12. Azure DevOps documentation // Microsoft. – URL: https://learn.microsoft.com/en-us/azure/devops (дата обращения: 22.04.2024).

13. Morales J. et al. Guide to implementing devsecops for a system of systems in highly regulated environments. – 2020.

14. Dileepkumar S. R., Mathew J. Optimize Continuous Integration and Continuous Deployment in Azure DevOps for a controlled Microsoft. NET environment using different techniques and

practices // IOP Conference Series: Materials Science and Engineering. – IOP Publishing, 2021. – Т. 1085. – №. 1. – С. 012027.

15. Vuppalapati C. et al. Automating tiny ml intelligent sensors devops using microsoft azure // 2020 ieee international conference on big data (big data). – IEEE, 2020. – С. 2375-2384.

16. Srithar S. et al. Cost-Effective Integration and Deployment of Enterprise Application Using Azure Cloud Devops // 2022 International Conference on Computer Communication and Informatics (ICCCI). – IEEE, 2022. – С. 01-05.