Сразу две критические уязвимости позволяют хакерам завладеть вашей сетью без особых усилий.

Исследователи по кибербезопасности опубликовали PoC (Proof-of-Concept) (доказательство концепции) — реализация метода и его демонстрация на практике, чтобы доказать, что концепция или теория работает." data-html="true" data-original-title="PoC" >PoC-Эксплойт (от англ. Exploit — означает «использовать что-то в своих интересах») — компьютерная программа, фрагмент программного кода или последовательность команд, которые используют ошибку или уязвимость для проведения атак на компьютерное ПО, аппаратное обеспечение или электронные устройства. Целью атаки является получение контроля над компьютерной системой, повышения привилегий или атака типа «отказ в обслуживании» (DoS или связанная с ней DDoS).

 Эксплойты обычно классифицируются и называются по: типу уязвимости, которую они используют; являются ли они локальными или удаленными; а также результатом запуска эксплойта (например, EoP, DoS, спуфинг). Одной из схем, предлагающих эксплойты нулевого дня, является Exploit-as-a-Service." data-html="true" data-original-title="Эксплойт" >эксплойт, демонстрирующий цепочку уязвимостей для удалённого выполнения кода (Remote Code Execution (RCE) — это критическая уязвимость, которая позволяет злоумышленнику дистанционно запустить вредоносный код в целевой системе по локальной сети или через Интернет. При этом физический доступ к устройству не требуется.

 В результате эксплуатации RCE-уязвимости киберпреступник может перехватить управление системой или ее отдельными компонентами, а также похитить конфиденциальные данные." data-html="true" data-original-title="RCE" >RCE) в Telerik Report Server – это программное решение для создания, управления и развертывания отчётов. Оно предоставляет пользователям инструменты для проектирования отчётов с помощью интуитивного конструктора, управления ими через централизованную веб-панель и развёртывания отчетов по расписанию или по запросу. Telerik Report Server поддерживает множество источников данных и форматов экспорта, что позволяет легко интегрироваться с различными системами и удовлетворять разнообразные потребности бизнеса в отчётности." data-html="true" data-original-title="Telerik Report Server" >Telerik Report Server от Progress Software Corporation — американская компания, специализирующаяся на разработке программного обеспечения и предоставлении инструментов для разработки и управления бизнес-приложениями.

 Компания была основана в 1981 году и предлагает широкий спектр продуктов, включая инструменты для разработки приложений, базы данных, интеграции данных и аналитических решений." data-html="true" data-original-title="Progress Software" >Progress Software.

Telerik Report Server — это комплексное решение для управления зашифрованными отчётами на базе API (Application Programming Interface) — это набор готовых функций и процедур, которые позволяют разработчикам создавать программное обеспечение, взаимодействующее с другими приложениями или сервисами. API определяет, как различные компоненты программного обеспечения должны взаимодействовать друг с другом, обеспечивая при этом безопасность и стабильность работы системы. API часто используется в веб-разработке для создания сайтов и приложений, которые используют данные и функциональность других сервисов." data-html="true" data-original-title="API" >API, которое организации используют для создания, совместного использования, хранения, распространения и планирования отчётов.

Исследователь по имени Сина Хейрха, при содействии коллеги по цеху Соруша Далили, разработал эксплойты и опубликовал подробное описание по эксплуатации сразу двух уязвимостей: обхода аутентификации и проблемы десериализации.

Уязвимость обхода аутентификации, отслеживаемая как CVE-2024-4358 с оценкой CVSS 9.8, позволяет создавать учётные записи администраторов без проверок. Хейрха обнаружил, что метод «Register» в «StartupController» доступен без аутентификации, что позволяет создавать учётные записи администратора сразу после завершения первоначальной настройки.

Эта проблема была устранена в обновлении Telerik Report Server 2024 Q2 10.1.24.514 от 15 мая, а 31 мая был опубликован бюллетень безопасности от команды Zero Day Iniative (Zero Day Initiative (ZDI) — это программа поиска и раскрытия уязвимостей, созданная компанией Trend Micro. Специалисты в рамках программы занимаются сбором информации об уязвимостях и ошибках в различных программных продуктах, включая операционные системы, браузеры, приложения и другие программы. Затем эта информация передается производителям программного обеспечения для исправления и защиты пользователей.

 ZDI следует стратегии «нулевого дня», что означает, что она ищет и раскрывает уязвимости ещё до их обнародования или использования злоумышленниками. Это позволяет разработчикам программного обеспечения исправить проблемы безопасности до того, как они станут широко известными и могут быть использованы во вред." data-html="true" data-original-title="ZDI" >ZDI).

Вторая уязвимость — CVE-2024-1800 с оценкой CVSS 8.8, позволяет удалённым аутентифицированным атакующим выполнять произвольный код на уязвимых серверах. Проблема была обнаружена ранее и сообщена вендору анонимным исследователем.

Используя эту уязвимость, потенциальный атакующий может отправить специально сформированный XML-пакет с элементом «ResourceDictionary» в кастомный десериализатор Telerik Report Server, который преобразует XML-элементы в .NET-типы. Специальный элемент в пакете затем использует класс «ObjectDataProvider» для выполнения произвольных команд на сервере, например, для запуска «cmd.exe».

Обновление безопасности было выпущено 7 марта 2024 года в версии Telerik Report Server 2024 Q1 10.0.24.305.

Хотя эксплуатация уязвимости десериализации сложна, описание и скрипт на Python от Хейрхи делают атаку достаточно понятной для потенциальных злоумышленников. Именно поэтому организациям рекомендуется как можно скорее применить доступные обновления, т.е. обновиться до версии 10.1.24.514 или выше, которые устраняют обе уязвимости.

Администраторам также рекомендуется проверить список пользователей на наличие новых учётных записей, добавленных по адресу»{host}/Users/Index», так как пока не зафиксировано случаев активной эксплуатации CVE-2024-4358.

Критические уязвимости в продуктах Progress Software редко остаются без внимания высококвалифицированных киберпреступников. Ярким примером служат масштабные атаки группы Clop , использовавшие уязвимость нулевого дня в платформе MOVEit Transfer. Эта вредоносная кампания затронула более 2770 жертв и косвенно повлияла почти на 96 миллионов человек, став одной из крупнейших операций по вымогательству в истории.

На перекрестке науки и фантазии — наш канал