CISA добавило уязвимость в свой каталог, призвав принять экстренные меры по защите федеральных систем.

В начале 2021 года в Apache – это название для семейства свободно распространяемых программных продуктов, которые разрабатываются и поддерживаются сообществом разработчиков. Они предназначены для создания различных типов веб-серверов, приложений и инструментов для работы с сетью.

 Проект Apache начался в 1995 году и на протяжении многих лет стал одним из самых популярных и влиятельных в мире открытого программного обеспечения.

 Apache предлагает широкий спектр продуктов, включая веб-сервер Apache HTTP Server, сервер приложений Apache Tomcat и многое другое. Эти продукты широко используются в веб-разработке, администрировании серверов и других областях информационных технологий." data-html="true" data-original-title="Apache" >Apache Flink была исправлена ошибка контроля доступа, которая теперь добавлена в каталог Cybersecurity and Infrastructure Security Agency (CISA) – это агентство, которое отвечает за защиту критической инфраструктуры США от киберугроз. Оно осуществляет мониторинг и анализ угроз, разрабатывает рекомендации по защите и обеспечивает техническую и информационную поддержку для организаций в этой отрасли. CISA также сотрудничает с другими правительственными агентствами и частным сектором для улучшения кибербезопасности в стране." data-html="true" data-original-title="CISA" >CISA Known Exploited Vulnerabilities (KEV) — это каталог известных эксплуатируемых уязвимостей, который ведётся агентством по кибербезопасности и защите инфраструктуры США (CISA). KEV представляет собой справочник уязвимостей, которые активно используются хакерами по всему миру.

 Каждая уязвимость, добавленная в этот каталог, должна быть устранена всеми федеральными гражданскими агентствами США в течение трех недель. Этот инструмент создан для обеспечения оперативного реагирования на реальные угрозы и своевременного устранения уязвимостей, прежде чем они будут эксплуатироваться нарушителями." data-html="true" data-original-title="KEV" >KEV. Это означает, что киберпреступники активно используют уязвимость для компрометации целей.

Apache Flink – это распределённый стриминговый и пакетный фреймворк для обработки данных и выполнения вычислений в реальном времени. Он предоставляет средства для анализа данных, поступающих в потоке, с минимальной задержкой, и поддерживает распределённую обработку на кластерах серверов. Flink используется для создания стриминговых приложений, а также для пакетной обработки данных, делая его универсальным инструментом для обработки данных в разнообразных сценариях." data-html="true" data-original-title="Apache Flink" >Apache Flink — это

платформа для потоковой и пакетной обработки данных с открытым исходным кодом, поддерживаемая Apache Software Foundation.

CVE-2020-17519 (оценка CVSS: 7.5) связана с неправильным контролем доступа, который позволяет злоумышленнику прочитать любой файл в локальной файловой системе JobManager через REST-интерфейс. Уязвимость затрагивает Apache Flink версии 1.11.0 (а также выпущенное в версиях 1.11.1 и 1.11.2).

Apache исправила уязвимость в версиях 1.11.3 и 1.12.0. Вскоре после этого исследователи по безопасности опубликовали PoC-код. И вот в мае 2024 года федеральные агентства и другие организации всё ещё используют небезопасные версии, а преступники активно используют уязвимость.

CISA не предоставила подробной информации об уязвимости и случаях эксплуатации. В базе данных статус ошибки обозначен как «неизвестный», то есть на данный момент не известно, кто злоупотребляет ошибкой и с какой целью. Несмотря на это, подразделение Palo Alto Networks Unit 42 предупредило о масштабных злоупотреблениях в период с ноября 2020 года по январь 2021 года.

Включение недостатка в каталог обязывает федеральные агентства либо закрыть брешь, либо полностью прекратить использование инструмента до 13 июня. Важно, чтобы и другие пользователи ПО убедились в наличии необходимых обновлений. Также рекомендуется проверить, не была ли система скомпрометирована через эту уязвимость. Несмотря на то, что об активной эксплуатации ошибки стало известно только сейчас, она могла быть использована и ранее.

На перекрестке науки и фантазии — наш канал