Исправьте CVE-2024-21683, пока преступники не добрались и до вашей сети.

Исследовательская команда SonicWall — это компания, специализирующаяся на обеспечении кибербезопасности. Она предлагает широкий спектр решений и продуктов для защиты сетей и данных от киберугроз. SonicWall разрабатывает и поставляет брандмауэры, антивирусные программы, системы обнаружения вторжений, VPN-решения и другие инструменты для защиты информации." data-html="true" data-original-title="SonicWall" >SonicWall обнаружила уязвимость в Atlassian — это австралийская технологическая компания, специализирующаяся на разработке программных продуктов для управления проектами, совместной работы и разработки программного обеспечения. Компания была основана в 2002 году и с тех пор стала одним из ведущих мировых поставщиков инструментов для разработчиков и команд, работающих в IT-сфере и не только." data-html="true" data-original-title="Atlassian" >Atlassian Atlassian Confluence — это современная платформа для совместной работы и управления знаниями в организации. Она предназначена для создания, хранения и совместного использования различных типов контента, таких как документы, вики-страницы, задачи и многое другое." data-html="true" data-original-title="Confluence" >Confluence Data Center и Server, приводящую к удалённому выполнению кода. Уязвимость идентифицирована как CVE-2024-21683 и имеет высокий CVSS балл — 8.3 из 10, что свидетельствует о значительной степени опасности.

Для эксплуатации уязвимости злоумышленнику необходимо иметь сетевой доступ к уязвимой системе и права на добавление новых языков макросов. Исследователи поясняют, что атака осуществляется путём загрузки поддельного JavaScript-файла с вредоносным кодом через функцию Configure Code Macro > Add A New Language.

Кроме того, для уязвимости уже существует рабочий PoC-эксплойт, что делает её ещё более опасной. Исследователи настоятельно рекомендуют пользователям обновить свои системы до последних версий, чтобы предотвратить возможные атаки.

Atlassian Confluence часто становится целью киберпреступников, так как платформа широко используется для корпоративного взаимодействия, разработки программного обеспечения и управления рабочими процессами. Она проникает глубоко в сетевые среды организаций, что делает её уязвимости особо привлекательными для злоумышленников.