Агентство подтвердило взлом своих систем, который передал химбезопасность США в руки хакеров.

Агентство 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 подтвердило январский взлом своей системы Chemical Security Assessment Tool (CSAT), в ходе которого хакеры взломали устройство Ivanti, что могло привести к утечке конфиденциальных данных.

CSAT используется предприятиями для отчета о наличии химических веществ, которые могут быть использованы для террористических целей. Если объект высокорисковый, система запрашивает загрузку оценки уязвимостей безопасности (Security Vulnerability Assessment, SVA) и плана безопасности химобъекта (Site Security Plan, SSP).

Первое сообщение о взломе CISA появилось в марте, когда агентство отключило два своих системных устройства для расследования инцидента. Хотя официальные лица CISA не раскрыли детали инцидента, источники сообщили, что речь идет об IP Gateway и Chemical Security Assessment Tool (CSAT).

CISA подтвердила, что на устройство Ivanti Connect Secure с 23 по 26 января 2024 года была загружена веб-оболочка. Несмотря на то, что все данные в приложении CSAT зашифрованы (AES 256), а кража данных не доказана, CISA уведомила компании и физические лица о повышенной осторожности.

В уведомлении агентства подчеркивается, что к информации мог быть получен неправомерный доступ. В том числе CISA рекомендует всем пользователям CSAT сменить пароли для любых своих учетных записей, использующих тот же пароль.

Хотя CISA не раскрыла, какие уязвимости были использованы, в документе агентства упоминается, что злоумышленники эксплуатировали несколько уязвимостей на устройствах Ivanti Connect Secure и Policy Secure Gateway. В частности, в документе указаны уязвимости CVE-2023-46805, CVE-2024-21887 и CVE-2024-21893, которые были раскрыты до взлома. Одна из уязвимостей, CVE-2024-21888, была раскрыта за день до взлома устройства Ivanti.

Несмотря на отсутствие доказательств утечки данных, количество потенциально затронутых лиц и организаций достигло уровня, соответствующего крупному инциденту (по закону о модернизации федеральной информационной безопасности FISMA). Кроме того, CISA работает над созданием колл-центра для пострадавших.

Потенциально подвергшиеся риску данные включают анкеты соискателей, оценки уязвимости безопасности, планы безопасности объектов, данные программы надежности персонала и личные данные пользователей CSAT, вплоть до номера паспортов и карт доступа с биометрией. Затронутые данные содержат критически важную информацию о состоянии безопасности и химическом инвентаре объектов, использующих инструмент CSAT. CISA не ответила на запросы о комментариях относительно того, кто стоял за атакой.

На перекрестке науки и фантазии — наш канал