Информзащита
Системный интегратор

РЕКОМЕНДАЦИИ ПО НЕЙТРАЛИЗАЦИИ УГРОЗЫ, СВЯЗАННОЙ С УЯЗВИМОСТЬЮ В «ДБО BS-CLIENT X64»

Компания «Информзащита» рекомендует всем организациям принять необходимые меры для защиты своих ресурсов и обеспечения информационной безопасности.

ОБЩЕЕ ОПИСАНИЕ УГРОЗЫ

Эксперты компании «Информзащита» обнаружили опасную уязвимость в программном обеспечении «ДБО BS-Client x64», которое используется финансовыми компаниями для организации дистанционного банковского обслуживания в различных режимах, например, «банк-клиент» или режим интернет-банка. Эксплуатация данной уязвимости не требует от злоумышленника высокой квалификации и может выполняться удаленно. Компания «Информзащита» рекомендует всем организациям принять необходимые меры для защиты своих ресурсов, персональных данных клиентов и их вкладов.

Уязвимость была обнаружена в ходе реализации проекта по анализу защищенности системы дистанционного банковского обслуживания одного из крупнейших банков, входящих в ТОП 50 банков России. Информация об уязвимости экспертами «Информзащиты» была отправлена разработчику, который подтвердил наличие такой проблемы и начал активно работать над исправлением ошибки.

ОПИСАНИЕ УЯЗВИМОСТИ

С помощью специально сформированного GET-запроса к интернет-приложению «ДБО BS-Client x64» сервер возвращает HTML-страницу со случайной информацией из области памяти, выделяемой под результат работы функции, в которой может содержаться конфиденциальная информация клиентов финансового учреждения, использующего систему онлайн-банка: ФИО клиента или название организации, номер счета, списки счетов и выписки по ним, последние транзакции, платежные поручения, остатки денежных средств и движения денег по счетам.

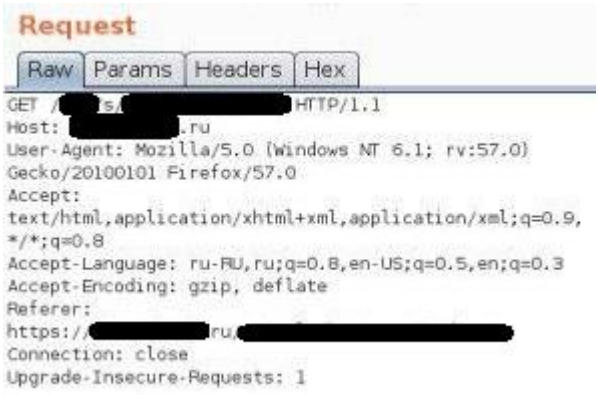

Рисунок 1. Пример GET-запроса

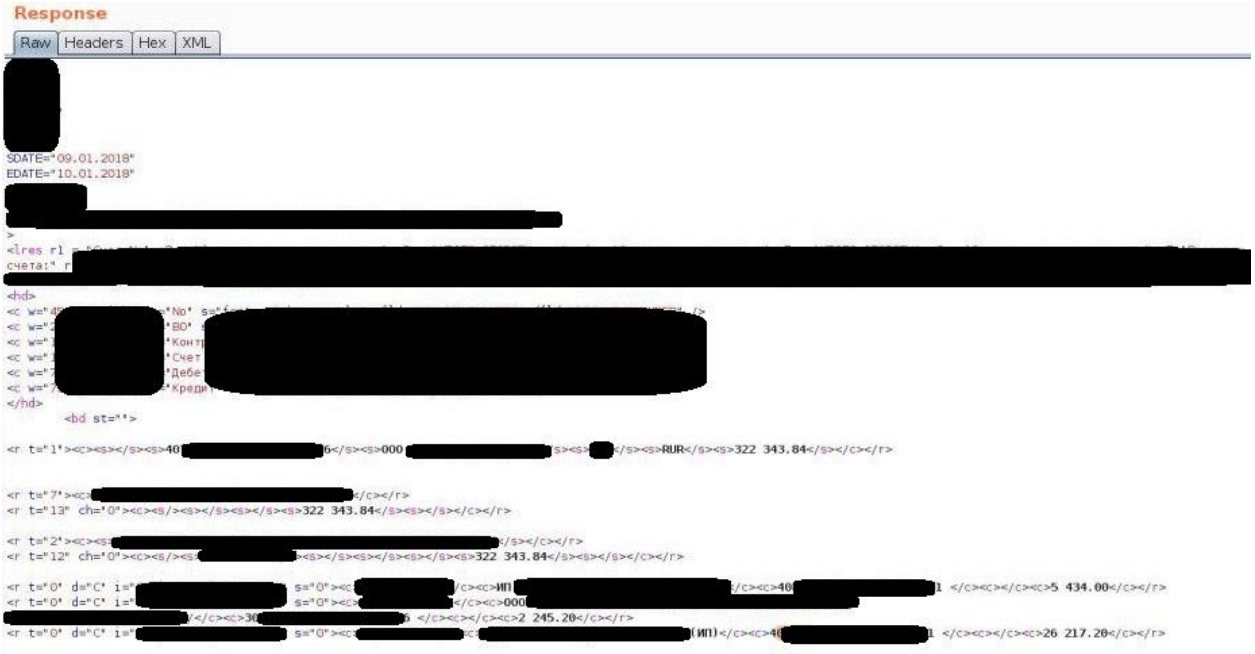

Рисунок 2. Пример ответа сервера в виде случайной HTML-страницы с конфиденциальной информацией

Помимо этого, выполнив данный GET-запрос у злоумышленников появляется возможность получить информацию об ошибках закрытых компонентов системы ДБО и отладочную информацию с помощью перебора определенных параметров.

Под угрозой находятся все финансовые учреждения, использующие уязвимые версии «ДБО BS-Client x64».

ПОСЛЕДСТВИЯ ЭКСПЛУАТАЦИИ УЯЗВИМОСТИ

Зная об этой уязвимости, киберпреступник может написать простейший скрипт, который будет в цикле посылать GET-запросы к приложению ДБО. Сервер банка возвращает случайную HTML-страницу, которая может содержать конфиденциальную банковскую информацию. У злоумышленников появляется возможность создания базы данных, которую можно использовать различными путями, например, для шантажа или выявления наиболее обеспеченных физических лиц и организации последующих целенаправленных атак на них.

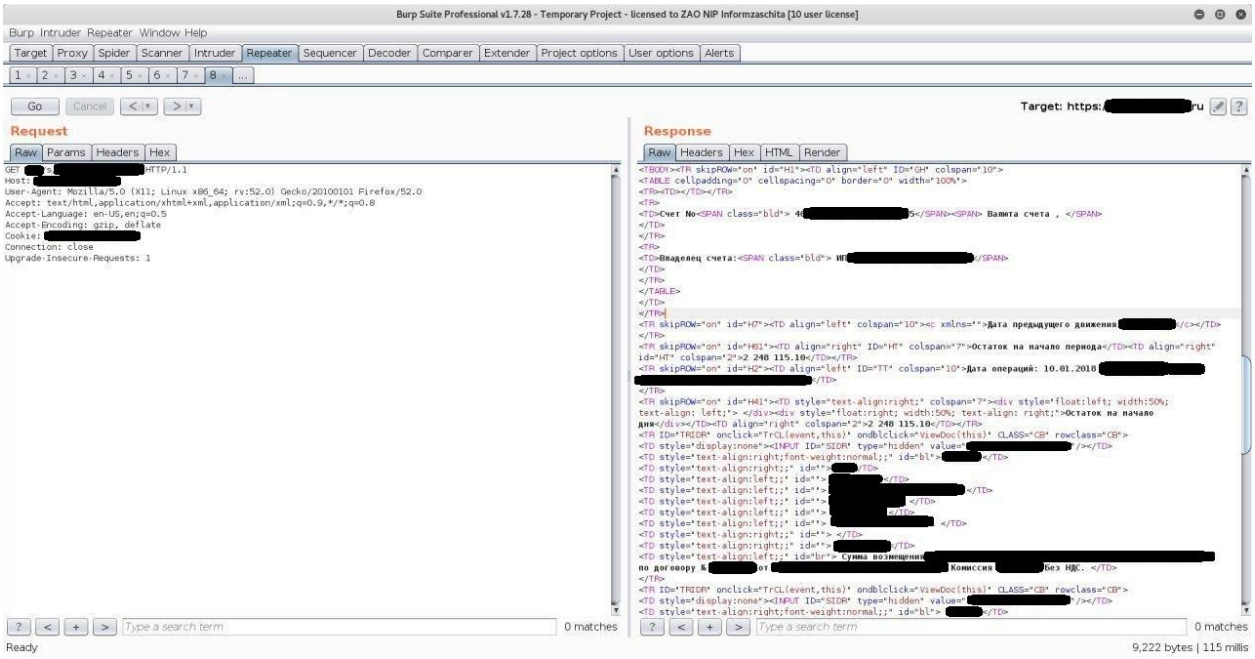

Рисунок 3. GET-запрос к уязвимому приложению и ответ сервера с конфиденциальной информацией

УЯЗВИМЫЕ ВЕРСИИ И РЕКОМЕНДАЦИИ

Данной уязвимости подвержены продукты всех версий «ДБО BS-Client x64» до 20.1.770 включительно. Для устранения недостатков эксперты «Информзащиты» рекомендуют обновить устаревшую версию продукта до 20.1.780 и регулярно проводить аудиты безопасности программного обеспечения и анализ кода приложений.

Команда экспертов «Информзащиты» готова проконсультировать все компании, обеспокоенные сложившейся ситуацией, по вопросам рисков и угроз, а также оперативно обеспечить защиту инфраструктуры:

www.infosec.ru
По услугам технической поддержки и сопровождения:
тел: +7 (495) 981-9222, +7 (495) 980-2345 доб. 06
e-mail: support@itsoc.ru

По услуге SOC — Security Operation Center:
Центр противодействия кибератакам IZ SOC:
8 (800) 100-23-55
тел: +7 (495) 980 2345
e-mail: soc@itsoc.ru