Новость · 13 января 2021, 11:36

Специалист по информационной безопасности обнаружил уязвимость в сети РЖД, позволяющую получить доступ к камерам компании по всей России

Специалист по информационной безопасности Алексей Сопов обнаружил уязвимость в сети РЖД, позволяющую получить доступ к камерам компании и электронным табло. Об этом он рассказал на портале «Хабр».

Сопов утверждает, что нашел в интернете открытый прокси-сервер и решил проверить, где он установлен. Автор указывает, что обычно открытый роутер — это либо взломанное устройство, либо владелец забыл отключить эту функцию.

Обнаружив уязвимость, Сопов решил найти владельца роутера, чтобы предупредить его. Просканировав *vpn*, как утверждает специалист, он обнаружил более 20 тысяч камер. «Огромное количество устройств с заводскими паролями», — подчеркивает автор.

При помощи кадров с камер наружного наблюдения Сопову удалось выяснить, что владелец сети — РЖД. По словам специалиста, при помощи уязвимости он смог получить доступ к камерам в офисах компании и на платформах по всей России, к «чему-то похожему» на систему мониторинга состояния систем обеспечения здания, системе

управления кондиционированием и вентиляцией, системам управления табло на перронах и другому сетевому оборудованию.

Автор предположил, что уязвимость могла появиться из-за «исходно плохой команды»: «Проверку проводил тот же отдел, который и проектировал или обслуживает систему. Отрицая проблему, они или сохраняют свою работу, или преследуют иные цели». Сопов добавил, что аудит мог проводить некомпетентный сотрудник или РЖД знает об уязвимости, но не хочет ее признавать.

Специалист уточнил, что, вероятно, он не первый, кто обнаружил уязвимость, так как «очень много признаков, что в этой сети кто-то "живет"».

В РЖД объявили о начатом расследовании из-за публикации. «Сообщаем, что утечки персональных данных клиентов холдинга не произошло, угрозы безопасности движения нет», — заверили в компании.