Обновляйтесь скорее, пока хакеры не проложили кибертропинку к вашему гаджету.

Вслед за уже привычным Patch Tuesday от Microsoft, компания Google – одна из крупнейших технологических компаний в мире, основанная в 1998 году в США. Основной продукт компании – поисковая система Google, которая позволяет находить информацию в интернете. Компания также разрабатывает множество других продуктов, таких как электронная почта Gmail, видеохостинг YouTube, карты Google Maps и операционную систему Android для мобильных устройств. Google является одним из лидеров в области искусственного интеллекта и облачных вычислений. Компания занимает высокие позиции в рейтингах лучших работодателей в мире.
" data-html="true" data-original-title="Google" >Google также выпустила обновления для устранения 50 уязвимостей безопасности в своих устройствах Pixel и предупредила, что одна из них, отслеживаемая как CVE-2024-32896, представляет собой ошибку повышения привилегий (EoP (Elevation of Privilege) или повышение привилегий – это тип уязвимости в программном обеспечении, который позволяет злоумышленнику повысить уровень своих привилегий или прав доступа в системе. Это означает, что атакующий, изначально имеющий ограниченные права, может получить доступ к более защищенным и важным функциям или данным. Обычно такие уязвимости используются для выполнения вредоносных действий, таких как изменение настроек системы, доступ к конфиденциальной информации или выполнение кода с привилегиями администратора." data-html="true" data-original-title="EoP" >EoP) и уже использовалась в реальных атаках в качестве Уязвимости нулевого дня (Zero-day, 0-day) — это программные недостатки, о которых производитель либо вообще не знает, либо знает, но ещё не успел выпустить патч для их устранения.

 Эти уязвимости представляют особый интерес для хакеров, так как они открывают возможности для скрытного проведения атак с низкой вероятностью обнаружения.

 Обычно такие уязвимости выявляются исследователями безопасности или непосредственно злоумышленниками. В первом случае информация о бреше безопасности обычно сообщается производителю для последующего исправления, во втором — уязвимость может быть эксплуатирована непосредственно в хакерских атаках." data-html="true" data-original-title="Zero-day" >Zero-day уязвимости.

«Есть признаки того, что CVE-2024-32896 уже могла быть использована ранее в ограниченных целевых атаках», — предупредила компания. «Все поддерживаемые устройства Google получат обновление до уровня патча 2024-06-05. Мы призываем всех пользователей Pixel незамедлительно установить эти обновления на свои устройства».

Google также отметила 44 других ошибки безопасности, непосредственно касающиеся устройств Pixel. Семь из них представляют собой уязвимости повышения привилегий и

считаются критическими.

Устройства Pixel, хотя и работают на Android, получают отдельные обновления безопасности и исправления ошибок, отличные от стандартных ежемесячных патчей, распространяемых для всех производителей Android-устройств. Это связано с их эксклюзивными функциями и возможностями, а также уникальной аппаратной платформой, контролируемой лично Google.

Более подробную информацию об июньских обновлениях для Pixel можно найти в бюллетене безопасности, посвящённом смартфонам Google. А чтобы применить обновление, пользователям Pixel необходимо перейти в «Настройки» > «Безопасность и конфиденциальность» > «Система и обновления» > «Обновление безопасности», нажать «Установить» и перезагрузить устройство для завершения процесса обновления.

В апреле Google также устраняла две другие 0day-уязвимости в Pixel, которые использовались судебно-экспертными фирмами для разблокировки телефонов без PIN-кода и доступа к данным. CVE-2024-29745 была помечена как уязвимость высокого уровня опасности, связанная с раскрытием информации в загрузчике Pixel, а CVE-2024-29748 — как уязвимость повышения привилегий в прошивке Pixel.