

ثغرة أمنية تسمح بامتلاك أجهزة آيفون عن بُعد



الأربعاء 2 ديسمبر 2020 04:12 م

كشف الباحث الأمني (إيان بير) Ian Beer من فريق جوجل الأمني Project Zero عن ثغرة أمنية تسمح بالتحكم الكامل في أجهزة آيفون عن بُعد دون أي تدخل من المستخدم

وأوضح أن مجموعة متنوعة من هواتف آيفون وأجهزة iOS الأخرى كانت عرضة حتى شهر مايو لاستغلال يسمح للمهاجمين بإعادة التشغيل عن بُعد والتحكم الكامل في أجهزتهم من مسافة بعيدة

ويسمح الاستغلال للمهاجم بقراءة رسائل البريد الإلكتروني والرسائل الأخرى، وتنزيل الصور، ومشاهدتك والاستماع إليك من خلال ميكروفون وكاميرا آيفون

وتستخدم أجهزة آيفون وآيباد وماك بروتوكولاً يسمى AWDL لإنشاء شبكات متداخلة لميزات، مثل: AirDrop و Sidecar، بحيث يمكنك إرسال الصور والملفات إلى أجهزة iOS الأخرى بسهولة وتحويل جهاز آيباد إلى شاشة ثانوية

واكتشف الباحث الأمني طريقة لاستغلال ذلك، كما وجد أيضاً طريقة لإجبار بروتوكول AWDL على التشغيل حتى لو تم إيقافه سابقاً

ويقول بير: إنه ليس لديه دليل على أن هذه المشكلات قد تم استغلالها، ويعترف بأن الأمر استغرق ستة أشهر كاملة للتعرف على هذا الاستغلال والتحقق منه وإثباته

وصحبت شركة آبل هذه الثغرة الأمنية اعتباراً من شهر مايو عبر iOS 13.5، لكن الباحث الأمني يقترح عدم الاستخفاف بوجود مثل هذا الاختراق

وقال: لا ينبغي أن تكون النتيجة الاستفادة من هذا المشروع أنه لا يوجد شخص قد يقضي ستة أشهر لمجرد اختراق هاتفي، وبدلاً من ذلك، يجب أن تكون النتيجة أن هناك شخصاً واحداً يعمل بمفرده كان قادراً على إيذاء مستخدمي آيفون بشكل خطير

ولا تشك آبل بوجود الاستغلال، واستشهدت بالباحث الأمني في سجلات التغييرات للعديد من تحديثات الأمان لشهر مايو 2020 المرتبطة بالثغرة الأمنية

وتشير الشركة إلى أن معظم مستخدمي iOS يستخدمون إصدارات أحدث من إصدارات iOS المصححة

وتوضح آبل أن الاختراق لن يعمل إلا عندما تكون في نطاق الشبكة اللاسلكية، وذلك بالرغم من أنك لست بحاجة إلى أن تكون ضمن الشبكة اللاسلكية نفسها