جوجل تكتشف ثغرة ضمن تطبيق الحماية ESET لنظام ماك

الأربعاء 1 مارس 2017 08:03 م

كشف باحثون يعملون في مجال الأمن والحماية يتبعون لشركة جوجل ثغرة أمنية في برنامج مكافحة الفيروسات ESET المبني خصيصاً لحماية نظام التشغيل ماكنتوش، بحيث يمكن استغلال هذا الخلل لتنفيذ هجمات وتعليمات برمجية عن بعد من خلال جذر أنظمة آبل ماكنتوش من خلال هجمات MITM.

وتمكن الباحث جيسون جيفنير والباحثة جان بي من اكتشاف ثغرة أمنية حرجة CVE-2016-9892 في تطبيق الحماية تسمح للقراصنة بمهاجمة أنظمة تشغيل ماك، بحيث يمكن عند استغلالها تنفيذ التعليمات البرمجية بصلاحية المدير مما يفتح باباً من احتمالات الأضرار التي لا حصر لها

ويوصف برنامج الحماية ESET Endpoint Antivirus 6 بحسب الشركة المصنعة له بانه مخصص للقضاء على جميع أنواع التهديدات الموجهة إلى نظام التشغيل ماكنتوش بما في ذلك الفيروسات والجذور الخفية والديدان وبرامج التجسس

وتكمن المشكلة في مكتبة تحليل XML القديمة المستخدمة من قبل التطبيق، والتي لا تقوم بإجراء عمليات فحص مصادقة الملقم بشكل مناسب، وخدمة esets_daemon التي تعمل بصلاحية المدير المرتبطة بإصدار قديم من مكتبة التحليل POCO XML.

ووفر هذا الخلل للقراصنة إمكانية اعتراض الطلبات المقدمة إلى المكتبة وايصال وثائق XML خبيثة باستخدام شهادات HTTPS موقعة ذاتياً، مما يمنح المهاجمين امتيازات المستخدم المدير لنظام ماكنتوش

وجرى إعداد التقرير الأصلي في شهر نوفمبر/تشرين الثاني الماضي، وأعطت جوجل شركة ESET ثلاثة أشهر لتسوية القضية قبل نشرها للوثائق الكاملة حول الثغرة في وقت سابق من هذا الأسبوع

وقدمت شركة الحماية لجوجل نسخة بناء مصححة من التطبيق للتحقق منها في شهر فبراير/شباط من هذا العام، لتصدر النسخة 6.4.168.0 لاحقاً للجمهور بعد تاكدها من إغلاق الثغرة