مايكروسوفت تطلق تحديثا ضخما لإصلاح 94 مشكلة أمنية

الاثنين 19 يونيو 2017 10:06 م

أعلنت شركة مايكروسوفت عن إطلاق تحديث ضخم بهدف ترقيع 94 ثغرة أمنية وإصلاح 27 مشكلة برمجية من شأنها السماح للمخترق بالتحكم عن بعد في آلة الضحية، ليصبح هذا واحدًا من أكبر التحديثات والترقيعات التي ستصلح ضعف الثغرات الأمنية التي تم إصلاحها في الشهرين الماضيين.

وأطلقت مايكروسوفت أيضًا إصلاحات أمنية تستهدف ترقيع الثغرات الموجودة في المنصات القديمة لارتفاع احتمالية اختراقها واستغلالها، وتوصي الشركة بوجوب تحديث أنظمة التشغيل في أقرب وقت ممكن، وتم ترقيع المنصات القديمة، بما في ذلك ويندوز إكس بي، وويندوز سيرفر 2003، وويندوز فيستا، وويندوز 8.

وطال التحديث الأمني كذلك الإصدارات الأقدم مثل:MS17-013، MS17-010، MS14-068، MS10-061، MS09-050، MS08-067، وترقيع الإصدارات الأحدث أيضًا مثل -CVE-2017-7269، CVE-2017-0267 to 0280، CVE-2017-0222، CVE-2017-0176، CVE-2017-8552، CVE-2017-8543، CVE-2017-8487، CVE-2017-8464، CVE-2017-8461.

وينصب الاهتمام في أغلب المنصات على نقطة الضعف CVE-2017-8543 والتي يتم استغلالها الآن بحسب مايكروسوفت، وهي الثغرة التي تمكن المهاجم من التحكم بحاسوب الضحية عن طريق إرسال طلب SMB لخدمة البحث الخاصة بنظام التشغيل ويندوز، وأثرت هذه المشكلة على نسخ ويندوز سيرفر 2016، 2012، 2008 بالإضافة إلى النسخ المكتبية مثل ويندوز 10 و7 و8.1، وهو ما جعل مايكروسوفت توفر ترقيعًا لهذه الثغرة لمنصات EOL القديمة، ولأنه يتم استغلال هذه الثغرة الآن في هجمات، فإننا نطلب من الشركات أن تبدأ في ترقيع أنظمتها في أقرب وقت ممكن.

ويوجد ثغرة أخرى يتم استغلالها وهي CVE-2017-8464 الموجودة في الإصدار Windows LNK وهي تسمح للمهاجم بالتحكم بشكل كامل في حاسوب الضحية.

بالإضافة إلى الثغرة ذات الأولوية المرتفعة CVE-2017-8527 وهي الثغرة الخاصة بخط مستخدم في محركات البحث، حيث يبدأ الهجوم عند تصفح المستخدم لموقع على الإنترنت يعمل بهذا الخط، وتتماثل الثغرتين CVE-2017-8528 و CVE-2017-0283 في مسألة الخط ويمكن استغلالهما إذا استعرض المستخدم نصوصًا ذات أكواد خاصة، وتسمح المشكلتان للمهاجم بالتحكم الكامل على حاسوب الضحية.

ويجب على الشركات التي تستخدم برنامج Outlook أن تقوم بترقيع CVE-2017-8507 وهي مشكلة أخرى تسمح للمهاجم بإرسال برمجيات خبيثة عبر البريد الإلكتروني والتحكم بشكل كامل عندما يستعرضها المستخدم داخل Outlook، ويمكن استغلال ثغرات أوفيس CVE-2017-0260 و CVE-2017-8506 عند فتح المستخدم لملف أوفيس مصاب ويجب أن يتم ترقيعها في أقرب وقت ممكن باعتبار أن أوفيس أكثر المنصات تعرضا لهجمات الهندسة الاجتماعية.

وتصلح ترقيعات مايكروسوفت إيدج وإنترنت إكسبلورر العديد من ثغرات التحكم عن بعد بالإضافة إلى CVE-2017-8498 و CVE-2017-8530 و CVE-2017-8523، والتي ذات أهمية كبيرة لأنه تم كشفها إلا أنها لم تستخدم في أي هجمات حتى الآن، ويوجد ثغرات تحكم تم إصلاحها اليوم بما فيها CVE-2017-0291 Windows PDF و CVE-2017-029.

وبشكل عام فإن هذا التحديث هو من أكبر التحديثات الأمنية، فهو يحمل ضعف التحديثات التي أطلقت خلال الشهرين الماضيين من حيث عدد الترقيعات، ومن شأن ثغرة CVE-2017-8543 SMB والترقيعات التي أطلقت لأنظمة التشغيل القديمة، إبقاء المسؤولين عن الأنظمة وفرق الأمن الرقمي مشغولين.