Como parte del martes de parches de septiembre de 2020, Microsoft lanzó un nuevo lote de actualizaciones de seguridad para corregir un total de 129 vulnerabilidades de seguridad recién descubiertas, que afectan a distintas versiones de sus sistemas operativos y software relacionado.

De los 129 errores que abarcan diversos productos como Microsoft Windows, Edge, Internet Explorer, ChakraCore, SQL Server, Exchange Server, Office, ASP.NET, OneDrive, Azure DevOps, Visual Studio y Microsoft Dynamics, 23 se catalogaron como críticos, 105 son importantes y uno es de gravedad moderada.

A diferencia de los últimos meses, ninguna de las vulnerabilidades de seguridad que parcheó la compañía en septiembre figura como públicamente conocida o bajo ataque activo hasta el momento.

La vulnerabilidad de corrupción de memoria (CVE-2020-16875) en el software de Microsoft Exchange, podría permitir a un atacante ejecutar código arbitrario en el nivel SYSTEM enviando un correo electrónico especialmente diseñado a un servidor Exchange vulnerable.

> *«Existe una vulnerabilidad de ejecución remota de código en el software Microsoft Exchange cuando el software no maneja correctamente los objetos en la memoria. Un atacante podría instalar programas, ver, cambiar o eliminar datos o crear nuevas cuentas»,* dijo Microsoft.

Microsoft también corrigió dos vulnerabilidades críticas de ejecución de código remoto en la biblioteca de códecs de Windows. Ambas existen en la forma en que la biblioteca de códecs de Microsoft Windows maneja los objetos en la memoria, pero mientras que una (CVE-2020-1129) podría explotarse para obtener información que comprometa más al usuario, la otra (CVE-2020-1319) podría utilizarse para tomar el control del sistema afectado.

Además, otras dos fallas de ejecución de código remoto afectan la implementación local de Microsoft Dynamics 365, pero ambas requieren que el atacante esté autenticado.

Microsoft también corrigió seis vulnerabilidades críticas de ejecución remota de código en SharePoint y una en SharePoint Server, esta última requiere autenticación.