Microsoft lanzó ayer su pack de actualizaciones de seguridad de software para el mes de julio de 2019, para parchear un total de 77 vulnerabilidades, de las cuales 14 están clasificadas como críticas, 62 son importantes y una es de gravedad moderada.

Las actualizaciones de seguridad incluyen parches para versiones compatibles de los sistemas operativos Windows y otros productos de Microsoft, como Internet Explorer, Edge, Office, Azure DevOps, software de código abierto, .NET Framework, Azure, SQL Server, ASP.NET, Visual Studio y Exchange Server.

Los detalles de 6 vulnerabilidades de seguridad, todos los que se calificaron como importantes, se hicieron públicos antes de que se lanzara el parche, ninguno se encontró siendo explotado por hackers.

Sin embargo, se ha informado que dos nuevas vulnerabilidades de escalamiento de privilegios, han sido explotadas activamente. Una afecta a todas las versiones compatibles del sistema operativo Windows y la otra a Windows 7 y Server 2008.

Ambas vulnerabilidades explotadas activamente conducen a la elevación de privilegios, una (CVE-2019-1132) reside en el componente Win32k y podría permitir que un atacante ejecute código arbitrario en modo kernel.

Otra vulnerabilidad de explotación activa (CVE-2019-0880), reside en la forma en que splwow64 (Thunking Spooler API) maneja ciertas llamadas, lo que permite a un atacante o un programa malicioso elevar sus privilegios en un sistema afectado de baja integridad a integridad media.

Las fallas conocidas públicamente afectan el tiempo de ejecución de Docker, la biblioteca criptográfica de SymCrypt de Windows, los servicios de escritorio remoto, la automatización de Azure, el servidor Microsoft SQL y el servicio de implementación de Windows AppX (AppXSVC).

Microsoft también lanzó actualizaciones para parchear 14 vulnerabilidades críticas, y como

se esperaba, todas llevaban a ataques remotos de ejecución de código y afectan a productos de Microsoft.

Algunas vulnerabilidades calificadas de importancia también conducen a ataques de ejecución remota de código, mientras que otras permiten la elevación de privilegios, la divulgación de información, los scripts entre sitios (XSS), la omisión de características de seguridad, la suplantación de identidad y los ataques de denegación de servicio.