Alerta de Seguridad Informática (9VSA-00014-001)

Nivel de Riesgo: Alto

Tipo: Vulnerabilidad

Fecha de lanzamiento original: 09 de Julio de 2019 | Última revisión 09 de Julio de 2019

Notificación

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

Microsoft lanzó hoy un conjunto de actualizaciones de seguridad de software para el mes de julio para parchear un total de 77 vulnerabilidades, 14 están clasificadas como críticas, 62 son importantes y 1 tiene una clasificación de gravedad moderada.

Vulnerabilidad

CVE-2019-0962 *	CVE-2019-1093	CVE-2019-1101
CVE-2019-1006 *	CVE-2019-1094	CVE-2019-1108
CVE-2019-1068 *	CVE-2019-1095	CVE-2019-1109
CVE-2019-1071	CVE-2019-1096	CVE-2019-1110
CVE-2019-1073	CVE-2019-1097	CVE-2019-1111
CVE-2019-1079	CVE-2019-1098	CVE-2019-1112
CVE-2019-1084	CVE-2019-1099	CVE-2019-1116
CVE-2019-1091	CVE-2019-1100	CVE-2019-1134

*incluyen pasos adicionales que deben ser considerados una vez se realice la actualización.

Impacto

Las actualizaciones de seguridad de julio de 2019 incluyen parches para varias 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.

De las vulnerabilidades de seguridad 6 se calificaron como importantes y se hicieron públicos antes de que se lanzara un parche, ninguna de estas se encontró siendo explotada.

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

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

La 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.

Productos afectados

Microsoft Windows
Internet Explorer
Microsoft Edge
Microsoft Office and Microsoft Office Services and Web Apps
Azure DevOps
Open Source Software
.NET Framework
Azure
SQL Server
ASP.NET
Visual Studio
Microsoft Exchange Server

Mitigación

Se recomienda encarecidamente a los usuarios y administradores de sistemas que apliquen los últimos parches de seguridad de Microsoft y mantengan actualizados sus sistemas, para así evitar que sean controlados y/o vulnerados por delincuentes informáticos.

Enlaces

https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/48293f19-d662-e911-a98e-000d3a33c573

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0962

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1006

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1068

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1071

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1073

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1079

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1084

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1091

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1093

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1094

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1095

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1096

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1097

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1098

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1099

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1100

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1101

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1108

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1109

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1110

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1111

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1112

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1116

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1134

Contactos

https://www.csirt.gob.cl
+ (562) 24863850
@CSIRTGOB
https://www.linkedin.com/company/csirt-gob