BOLETÍN DE ALERTA

Boletín Nro.: 2022-34
Fecha de publicación: 11/08/2022
Tema: Parches de seguridad de Microsoft soluciona vulnerabilidades Zero-Day

Algunos productos afectados:

- Active Directory Domain Services
- .NET Core
- Azure Batch Node Agent
- Azure Real Time Operating System
- Azure Site Recovery
- Azure Sphere
- Microsoft ATA Port Driver
- Microsoft Bluetooth Driver
- Microsoft Edge
- Microsoft Exchange Server

Para visualizar la lista detallada de los productos afectados ingrese al siguiente enlace.

Descripción:

Microsoft ha lanzado actualizaciones de seguridad para 121 vulnerabilidades incluyendo dos de Día Cero (*0-day*), que permitirían a un atacante realizar escalamiento de privilegios, denegación de servicio (*DoS*), ejecución remota de código (*RCE*), entre otros. Las principales se detallan a continuación:

- CVE-2022-34713, de severidad "alta", con una puntuación asignada de 7.8. Esta vulnerabilidad de Día Cero (*0-day*) explotada activamente, se debe a una falla en la herramienta Microsoft Windows Support Diagnostic Tool (*MSDT*). Un atacante remoto puede aprovechar esta vulnerabilidad para realizar escalamiento de privilegios en el sistema afectado.

- CVE-2022-30134, de severidad "alta", con una puntuación asignada de 7.6. Esta vulnerabilidad de Día Cero (*0-day*), se debe a un error en el control de datos de entrada de Microsoft Exchange. Un atacante remoto podría acceder a mensajes de correo electrónico específicos.

- CVE-2022-34691 de severidad "crítica", y sin puntuación asignada aún. Esta vulnerabilidad se debe a una falla en los servicios de *Active Directory*. Un atacante podría aprovechar esta vulnerabilidad para realizar escalamiento de privilegios en el sistema afectado.

Puede acceder a la lista completa de vulnerabilidades en el siguiente enlace.

Impacto:

La explotación exitosa de estas vulnerabilidades permitiría a un atacante realizar escalamiento de privilegios, ejecución remota de código (*RCE*), denegación de servicios (*DoS*), entre otros.

Solución:

Recomendamos instalar las actualizaciones correspondientes provistas por Microsoft a través de la siguiente guía:

- https://msrc.microsoft.com/update-guide/releaseNote/2022-Aug

Información adicional:

- https://www.bleepingcomputer.com/news/microsoft/microsoft-august-2022-patch-tuesday-fixes-exploited-zero-day-121-flaws/
- https://www.bleepingcomputer.com/microsoft-patch-tuesday-reports/August-2022.html
- https://msrc.microsoft.com/update-guide/
- https://nvd.nist.gov/vuln/detail/CVE-2022-34713
- https://nvd.nist.gov/vuln/detail/CVE-2022-30134
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34691
- https://msrc.microsoft.com/update-guide/
- https://msrc.microsoft.com/update-guide/releaseNote/2022-Aug