BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-66
Fecha de publicación: 20/11/2024
Tema: Múltiples vulnerabilidades críticas en Windows
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

- Múltiples productos de Microsoft
  - Microsoft Exchange Server
  - Active Directory Certificate Services
  - Windows Task Scheduler
  - SQL Server
  - Windows Update Stack
  - Entre otros

Descripción

Recientemente, **Microsoft** ha publicó un total de 89 vulnerabilidades, incluidas 4 consideradas **Zero-Days**: CVE-2024-43639, CVE-2024-49039, CVE-2024-49040 y CVE-2024-49019. Se reporta que las dos primeras están siendo explotadas activamente. Estas vulnerabilidades afectan a varios productos como Microsoft Exchange Server, Active Directory Certificate Services y Windows Task Scheduler.

De las vulnerabilidades publicadas por Microsoft en su parche mensual de los martes (**Microsoft November 2024 Patch Tuesday**), 4 fueron clasificadas como críticas, varias de ellas de ejecución remota de código (RCE).

A continuación, se detallan algunas de las vulnerabilidades más relevantes:

- **CVE-2024-43639** – Es una falla crítica de ejecución remota de código (**RCE**) que afecta al protocolo de autenticación Kerberos en Windows. Con una puntuación **CVSS de 9.8**, esta vulnerabilidad permite a un atacante no autenticado ejecutar código arbitrario en el sistema afectado mediante la explotación de una debilidad en el protocolo criptográfico de Kerberos. Aunque actualmente no se ha reportado explotación activa de esta vulnerabilidad, debido a su gravedad, se recomienda

encarecidamente aplicar las actualizaciones de seguridad proporcionadas por Microsoft para mitigar posibles riesgos.

- CVE-2024-49039 – Con una puntuación CVSS de 8.8, esta vulnerabilidad permite a los atacantes elevar sus privilegios desde un AppContainer de bajo privilegio, accediendo a un nivel de integridad más alto. Esto les permite ejecutar funciones RPC normalmente reservadas para cuentas privilegiadas, potencialmente comprometiendo los sistemas.

- CVE-2024-49040 – Esta vulnerabilidad (CVSS 7.5) en Microsoft Exchange Server permite a los atacantes suplantar la dirección de correo del remitente. La falla reside en la verificación de encabezados P2 y, con la última actualización de seguridad, los correos sospechosos ahora son marcados con una alerta de precaución en el cuerpo del mensaje.

- CVE-2024-49019 – Esta vulnerabilidad (CVSS 7.8) permite a los atacantes obtener privilegios de administrador de dominio abusando de plantillas de certificados versión 1. Microsoft ha recomendado revisar las configuraciones de certificados creados mediante plantillas que permitan a un amplio conjunto de usuarios o equipos inscribirse.

Puedes consultar la lista completa de CVE publicada por Microsoft en el siguiente enlace: Security Update Guide - Microsoft Security Response Center

Recomendamos aplicar las actualizaciones correspondientes para mitigar los riesgos asociados a estas vulnerabilidades lo más pronto posible, especialmente aquellas que están siendo explotadas activamente.

Solución

Es fundamental que los administradores de sistemas y usuarios finales apliquen estas actualizaciones de seguridad lo antes posible para proteger sus sistemas contra posibles explotaciones. Para obtener más detalles y acceder a las actualizaciones, visite el Centro de actualizaciones de seguridad de Microsoft.

Información adicional:

- Microsoft Releases November 2024 Patch Tuesday Updates
- Microsoft's November Patch Tuesday squashes several bugs in Windows 11 24H2 | ZDNET
- Microsoft Releases November 2024 Patch Tuesday Updates

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com