BOLETÍN DE ALERTA

Boletín Nro.: 2019-05
Fecha de publicación: 02/12/2019
Tema: Vulnerabilidad crítica en Windows permite a usuarios de bajos privilegios, poder escalar privilegios en el sistema operativo a usuario "SYSTEM".

- CVE-2019-1388

Sistemas afectados:

- Windows 7, 8, 10, Windows Server 2008, 2012, 2016, 2019 entre otros, puede ver la lista completa de los sistemas afectados aquí.

Descripción:

Eduardo Braun Prado, del equipo de ZDI (Zero Day Initiative) encontró una vulnerabilidad en la función del UAC (User Account Control), en español **Control de Cuentas de Usuarios,** de Windows bajo una funcionalidad conocida como Secure Desktop, la cual muestra una ventana al usuario para autenticarse cuando es necesario elevar privilegios en el sistema, con el fin de realizar funcionalidades que lo requieran, por ejemplo instalar software.

La falla existe porque en la ventana de diálogo mencionada anteriormente y en el identificador de objeto OID (Microsoft-specific object identifier) de Microsoft, no se chequean de manera adecuada los privilegios del usuario. Si un atacante hace clic en "Mostrar más detalles" en la ventana de diálogo del UAC, podrá ver el OID que se muestra en la pestaña de detalles como "SpcSpAgencyInfo", donde existe el problema. Parece ser que el cuadro de diálogo analiza el valor del OID y si encuentra datos válidos y en el formato correcto entonces en el campo de la ventana "Emitido por: " despliega los datos con un hipervínculo por lo cual al hacer clic en el hipervínculo, se abrirá un navegador desde el ejecutable conset.exe (archivo que inicia la interfaz del UAC) produciendo que dicho navegador se ejecute con privilegios de SYSTEM.

Puede ver una prueba de concepto aquí.

Impacto:

La vulnerabilidad permite a un usuario autenticado con bajos privilegios en el sistema poder acceder a privilegios de SYSTEM, comprometiendo de manera total el sistema.

Solución y Prevención:

Siempre es recomendable mantener nuestro software a la última versión estable disponible, en el siguiente enlace podrá encontrar la actualización que resuelve el problema para cada sistema operativo en particular:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1388

En caso de no poder aplicar la actualización, lo recomendable es limitar el acceso al símbolo del sistema y PowerShell para usuarios que no requieran utilizar explícitamente este tipo de funcionalidad dentro del sistema.

Información adicional:

- https://www.zerodayinitiative.com/blog/2019/11/19/thanksgiving-treat-easy-as-pie-windows-7-secure-desktop-escalation-of-privilege
- https://nvd.nist.gov/vuln/detail/CVE-2019-1388
- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1388