BOLETÍN DE ALERTA

Boletín Nro.: 2021-32

Fecha de publicación: 26/11/2021

Tema: Vulnerabilidad de elevación de privilegios de Windows Installer.

Versión afectada:

- Microsoft Windows 8 y superior.
- Microsoft Windows Server 2022.

Descripción:

La vulnerabilidad identificada como CVE-2021-41379 con una puntuación alta de 7.8, corresponde a una falla del Windows Installer que permite la elevación de privilegios, la cual puede ser explotada a través de una cuenta con privilegios mínimos. Inicialmente un atacante solo podría eliminar archivos específicos en un sistema, sin embargo, el parche que Microsoft ha publicado para subsanar dicha vulnerabilidad, no ha solucionado la misma, lo que ha permitido al investigador Abdelhamid Naceri evadir las medidas de seguridad implementadas en dicho parche.

El código que lanzó Naceri aprovecha la lista de control de acceso discrecional (DACL) para Microsoft Edge Elevation Service con el fin de reemplazar cualquier archivo ejecutable en el sistema con un archivo MSI, lo que permite a un atacante ejecutar código malicioso como administrador. Actualmente Microsoft no se ha pronunciado sobre estos reportes.

Impacto:

Esta nueva variante brinda a los usuarios la capacidad de elevar los privilegios locales a privilegios de administrador (*System)*. Una vez obtenido, los desarrolladores de *malware* pueden usar estos privilegios para reemplazar cualquier archivo ejecutable en el sistema con un archivo MSI para luego ejecutar el código malicioso con privilegios de administrador.

Detección:

Implementar una regla Snort (SID 58635 y 58636) que mantendrán a los usuarios protegidos de la explotación de esta vulnerabilidad.

Snort - Network Intrusion Detection & Prevention System

Solución:

- Actualmente aún no se encuentra con alguna solución y/o parche oficial a la vulnerabilidad.

Información adicional:

- https://www.snort.org/advisories/talos-rules-2021-11-23
- https://nvd.nist.gov/vuln/detail/CVE-2021-41379
- CVE - CVE-2021-41379 (mitre.org)
- CVE-2021-41379 - Security Update Guide - Microsoft - Windows Installer Elevation of Privilege Vulnerability