La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), agregó el viernes 10 nuevas vulnerabilidades explotadas activamente a su Catálogo de Vulnerabilidades Explotadas Conocidas (KEV), incluyendo una vulnerabilidad de seguridad de alta gravedad que afecta al software de automatización industrial Delta Electronics.

El problema, rastreado como CVE-2021-38406 (puntaje CVSS: 7.8), afecta a las versiones 2.00.07 y anteriores de DOPSoft 2. Una explotación exitosa de la falla podría conducir a la ejecución de código arbitrario.

> *«Delta Electronics DOPSoft2 carece de la validación adecuada de los datos proporcionados por el usuario al analizar archivos de proyectos específicos (validación de entrada incorrecta), lo que resulta en una escritura fuera de los límites que permite la ejecución del código»,* dijo CISA.

Cabe mencionar que CVE-2021-38406 se divulgó originalmente como parte de un aviso de sistemas de control industrial (ICS) publicado en septiembre de 2021.

Sin embargo, no hay parches que aborden la vulnerabilidad, y CISA dijo que *«el producto afectado está al final de su vida útil y debe desconectarse si todavía está en uso».* Las agencias del Poder Ejecutivo Civil Federal (FCEB) tienen el mandato de seguir la directriz antes del 15 de septiembre de 2022.

No existe mucha información disponible sobre la naturaleza de los ataques que explotan el error de seguridad, pero un informe reciente de Unit42 de Palo Alto Networks señaló instancias de ataques en estado salvaje que aprovecharon la vulnerabilidad entre febrero y abril de 2022.

El desarrollo agrega peso a la noción de que los adversarios se están volviendo más rápidos en la explotación de vulnerabilidades recién publicadas cuando se divulgan por primera vez, lo que lleva a intentos de escaneo indiscriminados y oportunistas que tienen como objetivo aprovechar la aplicación retrasada de parches.

Estos ataques cibernéticos por lo general siguen una secuencia específica de explotación que involucra web shells, criptomineros, botnets y troyanos de acceso remoto (RAT), seguidos de intermediarios de acceso inicial (IAB) que allanan el camino para el ransomware.

Entre otros defectos explotados activamente se encuentran:

- CVE-2022-26352: Vulnerabilidad de carga de archivos sin restricciones de dotCMS
- CVE-2022-24706: Vulnerabilidad de inicialización predeterminada insegura de recursos de Apache CouchDB
- CVE-2022-24112: Vulnerabilidad de omisión de autenticación APISIX de Apache
- CVE-2022-22963: Vulnerabilidad de ejecución remota de código de la función Spring Cloud de VMware Tanzu
- CVE-2022-2294: Vulnerabilidad de desbordamiento del búfer de pila de WebRTC
- CVE-2021-39226: Vulnerabilidad de omisión de autenticación de Grafana
- CVE-2020-36193: Vulnerabilidad de resolución de enlace inadecuado de PEAR Archive_Tar
- CVE-2020-28949: PEAR Archive_Tar Deserialización de vulnerabilidad de datos no confiables

Vulnerabilidad de iOS y macOS agregada a la lista

Otra vulnerabilidad de alta gravedad agregada al Catálogo KEV es CVE-2021-31010 (puntuación CVSS: 7.5), un problema de deserialización en el componente Core Telephony de Apple, que podría aprovecharse para eludir las restricciones de sandbox.

La compañía también abordó la vulnerabilidad en iOS 12.5.5, iOS 14.8, iPadOS 14.8, macOS Big Sur 11.6 (y Security Update 2021-005 Catalina) y watchOS 7.6.2 lanzados en septiembre de 2021.

Aunque no había indicios de que se estuviera explotando la vulnerabilidad en ese momento, Apple parece haber revisado de forma silenciosa sus avisos el 25 de mayo de 2022 para agregar la vulnerabilidad y confirmar que efectivamente se había abusado de ella en los

ataques.

> *«Apple estaba al tanto de un informe de que este problema podría haber sido explotado activamente en el momento del lanzamiento»*, dijo la compañía y atribuyó el descubrimiento a Citizen Lab y Google Project Zero.

La actualización de septiembre también se destaca por remediar CVE-2021-30858 y CVE-2021-30860, ambos empleados por NSO Group, los creadores del software espía Pegasus, para sortear las características de seguridad de los sistemas operativos.

Esto sugiere que existe la posibilidad de que CVE-2021-31010 se haya unido a las dos vulnerabilidades mencionadas en una cadena de ataque para escapar de la zona de pruebas y lograr la ejecución de código arbitrario.