ALERTA DE SEGURIDAD

CSIRT-RD

Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

FECHA DE PUBLICACIÓN: 30 DE MARZO 2023

PRESIDENCIA DE LA REPÚBLICA DOMINICANA
MINISTERIO DE LA PRESIDENCIA

CNCS CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

CSIRT-RD
Equipo Nacional de Respuestas a Incidentes Cibernéticos del CNCS

El presente documento es propiedad del **Centro Nacional de Ciberseguridad (CNCS)**, y fue generado mediante el análisis de varias fuentes de terceras partes y una investigación del equipo CSIRT-RD.

ALERTA DE SEGURIDAD

- **TLP:** CLEAR
- **Tipo de incidente:** Malware
- **Categoría:** Código Malicioso
- **Nivel de peligrosidad: ALTO**

DETALLES DE ALERTA

El Equipo Nacional de Respuesta a Incidentes Cibernéticos de la República Dominicana (CSIRT-RD) ha identificado una campaña de compromiso a través del proveedor de soluciones de comunicaciones empresariales **3CX**, donde este último ha llegado hacer objeto de un **ataque de cadena de suministro** en el que los ciber atacantes han logrado comprometer su aplicación de escritorio "**3CX Phone**". El ataque permitió a los ciberdelincuentes inyectar malware en la aplicación, lo que les propició controlar remotamente las computadoras de los usuarios. Se, el ataque se llevó a cabo mediante la explotación de una vulnerabilidad en un software de terceros utilizado por el proveedor.

INDICADORES DE COMPROMISO (IoC)

Dominios

akamaicontainer[.]com
akamaitechcloudservices[.]com
azuredeploystore[.]com
azureonlinecloud[.]com
azureonlinestorage[.]com
officeaddons[.]com
officestoragebox[.]com
dunamistrd[.]com
glcloudservice[.]com
journalide[.]org
msedgepackageinfo[.]com
msstorageazure[.]com
msstorageboxes[.]com
pbxcloudeservices[.]com
pbxsources[.]com
qwepoi123098[.]com
sbmsa[.]wiki
sourceslabs[.]com
visualstudiofactory[.]com
zacharryblogs[.]com
pbxphonenetwork[.]com

VULNERABILIDADES

El CSIRT-RD ha identificado mediante labores de observación de diversas fuentes de inteligencia de amenaza que la vulnerabilidad aprovechada en cuestión pudiera haber sido aprovechada por un fallo en la inyección de código en el software utilizado provisto por el proveedor. Un actor de amenaza pudo llegar explotar esta vulnerabilidad en un software de terceros que se encontraba integrado para lograr inyectar código malicioso en la aplicación de escritorio, que posteriormente les permitió el tomar el control remoto de las computadoras donde había llegado a ser descargado el aplicativo.

Hasta el momento de esta publicación, el ataque en cuestión pudiese haber sido llevado a cabo por la identificación de una vulnerabilidad por parte de los ciberdelincuentes en un software de terceros que era utilizado por la aplicación, donde luego pudo llegar la carga de un código malicioso en la aplicación de escritorio de **3CXDesktopApp** a través de la modificación de este código, una vez que los usuarios descargaban e instalaban la aplicación de escritorio comprometida, el código inyectado comenzaba a ejecutarse dentro del proceso y los atacantes podían lograr controlar remotamente la computadora víctima del ataque.

Es importante destacar que los atacantes pudieron haber comprometido la aplicación de escritorio del proveedor, debido a que misma confiaba en un software de terceros integrado que resultaba ser vulnerable. Este tipo de vulnerabilidad es conocida como **'cadena de suministro'**, y subraya la importancia de verificar cuidadosamente la seguridad de los proveedores y los softwares de terceros utilizados en los sistemas empresariales.

RECOMENDACIONES

1. **Realizar** el análisis correspondiente para el bloqueo a los indicadores de compromiso expuestos (indicados previamente) por un mínimo de 30 días.
2. **Realizar** una actualización de forma inmediata de los aplicativos instalados a las últimas versiones estables que se encuentren disponibles y publicadas por parte del proveedor de 3CX.
3. **Mantener** un monitoreo continuo sobre todos los equipos y servicios tecnología que se encuentren en uso en la organización.
4. **Realizar** contacto inmediato con el Equipo Nacional de Respuesta a Incidentes Cibernéticos (CSIRT-RD), a través del correo incidentes@csirt.gob.do, para reportar cualquier acción sospechosa o posible incidente de ciberseguridad antes de realizar una acción.
5. **Realizar** campañas de concientización periódica a todos los usuarios de la institución.

El Equipo Nacional de Respuesta a Incidentes Cibernéticos de la República Dominicana (CSIRT-RD) del Centro Nacional de Ciberseguridad (CNCS) emite esta alerta de seguridad mediante las funciones establecidas en el decreto presidencial 230-18 y 313-22 que regula la Estrategia Nacional de Ciberseguridad, asimismo como parte de las atribuciones designadas en el decreto 685-22 sobre "Notificación obligatoria de incidentes e intercambio de inteligencia de amenazas cibernéticas".