# Vulnerabilidades en el Ciberespacio Dominicano

## Servicio de Escritorio Remoto (RDP)

CNCS | CENTRO NACIONAL DE CIBERSEGURIDAD
REPÚBLICA DOMINICANA

CSIRT-RD

# Vulnerabilidades en el Ciberespacio Dominicano

## Servicio de Escritorio Remoto (RDP)

**Edición:** 01

Centro Nacional de Ciberseguridad (CNCS)
Centro Nacional de Respuesta a Incidentes Cibernéticos de la República Dominicana (CSIRT-RD)
Fecha de Publicación: 08 de Mayo 2020
Diagramación: SAORGA, S.R.L.

## SOBRE EL CNCS

El Centro Nacional de Ciberseguridad es una entidad dedicada al desarrollo de la ciberseguridad, al fortalecimiento de la confianza digital del usuario dominicano y a la protección de la infraestructura crítica y tecnológica del Estado dominicano.

## MISIÓN

Velar por el establecimiento de los mecanismos adecuados de ciberseguridad que protejan al Estado, a los ciudadanos y a los sectores productivos, para el desarrollo y la seguridad nacional a través de la continuidad, actualización y evaluación de la Estrategia Nacional de Ciberseguridad, la formulación de políticas derivadas de dicha estrategia y la definición de las iniciativas, programas y proyectos que lleven a la realización exitosa de la misma, así como la prevención, detección y gestión de incidentes generados en sistemas de información del gobierno y en las infraestructuras críticas nacionales.

## VISIÓN

Ser un ente de referencia en el establecimiento de las mejores prácticas de aseguramiento del ciberespacio dominicano.

## VALORES

Compromiso | Ética | Honestidad

# INTRODUCCIÓN

El presente documento muestra los resultados del trabajo de investigación realizado por el Centro Nacional de Ciberseguridad (CNCS), en relación a la ciberexposción del servicio de escritorio remoto (RDP) de Windows.

A modo de introducción se define el protocolo remoto de escritorio conocido por sus siglas en inglés (RDP); un servicio que permite a las máquinas conectarse y administrar recursos en una computadora remota. Para establecer una sesión RDP, una máquina cliente envía una solicitud de conexión a través de la red a una máquina host en el puerto TCP estándar 3389.

El protocolo RDP ha sido clasificado como un indicador de ciberexposición y hoy en día presenta vulnerabilidades comúnmente conocidas que afectan varias versiones del sistema operativo Microsoft.

| INDICADOR | VULNERABILIDAD |
|---|---|
| CIBEREXPOSICIÓN | BLUEKEEP |

El 14 de mayo de 2019, Microsoft lanzó una actualización crítica para corregir una vulnerabilidad de ejecución de código remoto, debido al manejo inadecuado de solicitudes en el servicio RDP. Esta vulnerabilidad conocida como (CVE-2019-0708) no requiere autenticación ni la interacción del usuario para ser explotado. Se puede explotar simplemente enviando un paquete diseñado para el sistema de destino a través de RDP.

# VULNERABILIDADES EN EL CIBERESPACIO DOMINICANO ABRIL - 2020

BlueKeep es una vulnerabilidad crítica en el servicio de escritorio remoto que afecta varios sistemas de Windows.  La complejidad de explotación es relativamente baja. El servicio de escritorio remoto de Windows es muy demandado y bastante expuesto, según datos del motor de búsqueda Shodan, en la actualidad, se encuentran más de cuatro millones de dispositivos accesibles a RDP en todo el mundo. Por tanto, los ciberatacantes podrían identificar los hosts vulnerables a bluekeep y desencadenar una ola de ataques de ransomware que afectarían millones de dispositivos.

Esta vulnerabilidad, registrada como CVE-2019–0708[1], describe la posibilidad de que un ciberatacante intente conectarse al sistema destino mediante el Protocolo de Escritorio Remoto (RDP) y al enviar un paquete especialmente diseñado, un atacante puede establecer el valor del ID del canal a uno diferente que el servicio RDP no espera, lo que provoca un error de corrupción de memoria que crea las condiciones para que se produzca la ejecución remota de código. Si el atacante decide continuar con los paquetes diseñados para aprovechar esta falla, la ejecución remota de código se puede lograr con privilegios de usuario del sistema.

## SISTEMAS AFECTADOS POR EL CVE-2019-0708

- Microsoft Windows 7 (SP1).
- Microsoft Windows Server 2003 (SP2).
- Microsoft Windows Server 2008 (SP1).
- Microsoft Windows Vista (SP2).
- Microsoft Windows XP (SP2, SP3).

## SISTEMAS AFECTADOS POR EL CVE-2019-0708

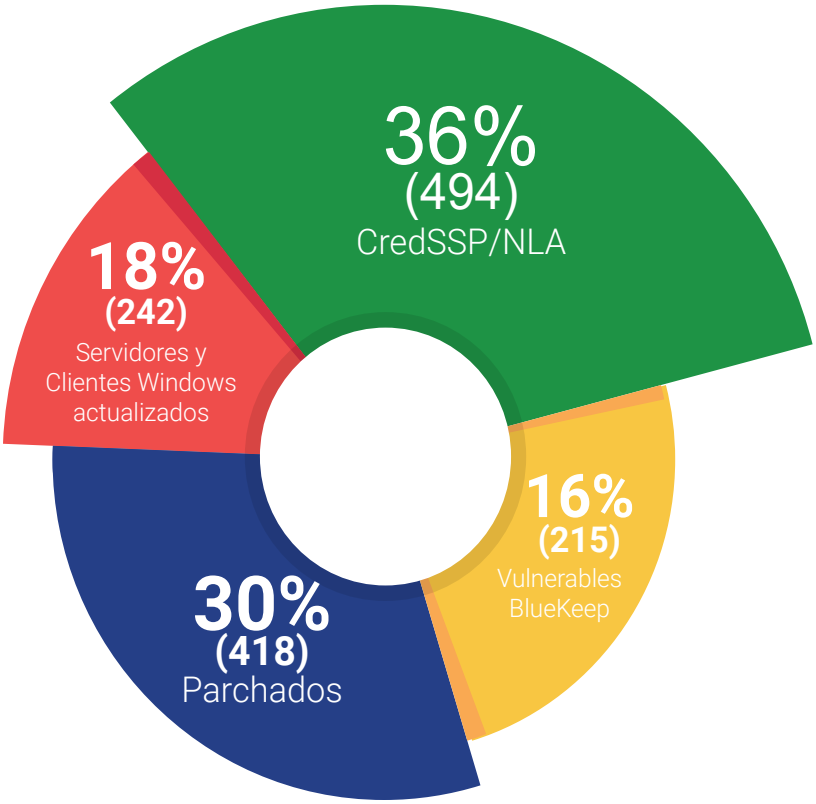
El Equipo Nacional de Repuesta a Incidentes Cibernéticos (CSIRT-RD), a través del Observatorio Nacional de Ciberseguridad, ha monitoreado la ciberexposición del servicio de escritorio remoto de Windows en la República Dominicana, en el período comprendido Enero - Abril 2020. En consecuencia, se identificaron una cantidad importante de dispositivos que se encuentran actualmente expuestos a internet y vulnerables al CVE-2019–0708.

Para lograr cuantificar los servicios de escritorio remoto expuestos a internet, el CSIRT-RD realizó un escaneo -no invasivo- al bloque de direcciones IP asignadas a la República Dominicana, evidenciando que 1,369 direcciones IP (hosts) poseen servicios de RDP disponibles en el puerto por defecto 3389.

1 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708

En ese mismo sentido, se determinó que más de 200 dispositivos se encuentran vulnerables a Bluekeep y actualmente están accesibles desde internet, representando un 16% del total de los servicios expuestos.

## EXPOSICIÓN DE SERVICIOS DE RDP EN EL CIBERESPACIO DOMINICANO




De igual manera, se observaron 418 hosts que han sido actualizados y la vulnerabilidad ha sido remediada. Con respecto a la autenticación de nivel de red, conocida por sus siglas en inglés NLA (Network Level Authentication), utilizada en RDP y sugerida por Microsoft, en caso de que el servidor sea crítico y no exista la posiblidad de parcharlo de inmediato, el estudio reveló que 494 host dominicanos han habilitado CredSSP/NLA.

Por otro lado, el 18% de los hosts analizados correspondieron a servidores de Microsoft Windows actualizados no vulnerables y Windows con protección de salida hacia internet (IPS / IDS).

| CATEGORÍA | CANTIDAD |
|---|---|
| Servidores y Clientes Windows actualizados | 242 |
| CredSSP/NLA | 494 |
| Parchados | 418 |
| Vulnerables BlueKeep | 215 |
| **TOTAL ACCESIBLES RDP** | **1369** |

**Tabla 1.** Accesibles RDP en el ciberespacio dominicano Abril-2020.

## IMPACTO

| | |
|---|---|
| **Vector de acceso:** | A través de red |
| **Complejidad de Acceso:** | Baja |
| **Autenticación:** | No requerida para explotarla |
| **Tipo de impacto:** | Compromiso total de la integridad del sistema<br>Compromiso total de la confidencialidad del sistema<br>Compromiso total de la disponibilidad del sistema |

## PROTOCOLO RDP – Técnica (DLL Side-Loading)

El 21 de abril de este año, investigadores de seguridad de la empresa Cymulate[1] descubrieron una nueva técnica de evasión que permitiría ejecutar código malicioso utilizando el Protocolo de Escritorio Remoto (RDP) de Microsoft, utilizando la técnica de carga lateral de DLL. Mientras analizaban MSTSC y RDP, observaron esta técnica única que permite a los atacantes eludir los controles de seguridad. Un sistema de Windows que ejecuta RDP utiliza el Cliente de Servicios de Terminal Server de Microsoft (MSTSC) y este MSTSC se basa en un archivo DLL (mstscax.dll). Cymulate identificó que "Microsoft Terminal Services Client (MSTSC) realiza la carga retardada de mstscax.dll con un comportamiento que puede provocar que un atacante pase por alto los controles de seguridad. El ejecutable carga explícitamente "mstscax.dll" sin verificaciones de integridad para validar el código de la biblioteca".

Un atacante podría usar este punto ciego para reemplazar el "mstscax.dll" que está presente en la carpeta "C:\Windows\System32" o copiándolo en una carpeta externa que no requiere privilegios de administrador.

Para mitigar esta amenaza, se recomienda a los usuarios deshabilitar el uso de mstsc.exe y monitorear el comportamiento anormal malicioso.

## PROTECCIÓN / MITIGACIÓN

Actualizar / instalar los parches de seguridad, recomendados por Microsoft, para la vulnerabilidad de bluekeep disponibles para Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008 y Windows Server 2008 R2.

1 https://cymulate.com/news/cymulate-discovers-hidden-malware-mstsc/

- Windows® XP / Windows Server® 2003 – Parche de seguridad KB4500331
- https://www.catalog.update.microsoft.com/Search.aspx?q=KB450033Windows® Vista / Windows Server® 2008 – Parche de seguridad KB4499180 OR Monthly Rollup KB4499149 https://support.microsoft.com/en-us/help/4499149/windows-server-2008-update-kb4499149
- Windows® 7 / Windows Server® 2008 R2 – Parche de seguridad KB4499175 OR Monthly Rollup KB4499164 https://www.catalog.update.microsoft.com/Search.aspx?q=KB4499164

Al mismo tiempo, se recomienda limitar las conexiones RDP entre equipos dentro de una misma red:

- Aplicación de segmentación de red adecuada.
- Denegar estaciones de trabajo estándar que permitan la conexión arbitraria entre servidores o dispositivos por medio RDP.
- Limitar el acceso RDP únicamente a servidores; recomendamos considerar el uso de un jump box para la conexión entre los mismos.

**Habilitar la Autenticación de Nivel de Red (NLA) para RDP.** Network Level Authentication ofrece una capa adicional de protección. Cuando está habilitado, un usuario que intenta conectarse a un sistema remoto a través de RDP necesitará autenticar su identidad en primer lugar, antes de que se establezca una sesión.

Servicios de escaneos en internet, hacen posible que ciberatacantes encuentren sistemas expuestos a Internet con RDP accesibles. Cambiar el puerto RDP asegura que los programas que habitualmente escanean estos puertos que buscan RDP abiertos, no sean encontrados.

**Utilizar una puerta de enlace RDP.** Las puertas de enlace RDP normalmente se instalan dentro de la red corporativa. La función de una puerta de enlace permite pasar de forma segura el tráfico hacia y desde un cliente remoto a un dispositivo local. Puede ayudar a las organizaciones a garantizar que solo los usuarios autorizados puedan usar RDP y controlar los dispositivos a los que tienen acceso. El uso de una puerta de enlace RDP puede evitar o minimizar el acceso de usuarios remotos y dar a las organizaciones un mayor control sobre las funciones de los usuarios, los privilegios de acceso, y los requisitos de autenticación.

# GLOSARIO

**DLL:** La biblioteca de vínculos dinámicos (DLL) es la implementación por parte de Microsoft del concepto de biblioteca compartida en los sistemas operativos Microsoft Windows y OS/2. Estas bibliotecas suelen tener la extensión de archivo , (para bibliotecas que contienen controles ActiveX) o (para controladores de sistema heredados).

**Higiene digital:** Es el uso responsable de las herramientas tecnológicas que se nos brindan, la misma refiere mantener una exposición mínima sobre internet.

**Ciberdelincuente:** Personas  que intenta sacar ventaja de los fallos de sistemas y humanos donde estos se logran beneficiar monetariamente o por venganza.

**Parches:** Los parches de seguridad solucionan agujeros de seguridad y, siempre que es posible, no modifican la funcionalidad del programa; son especialmente frecuentes en aplicaciones que interactúan con Internet.

**IPS:** Un sistema de prevención de intrusos (o por sus siglas en inglés IPS) es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

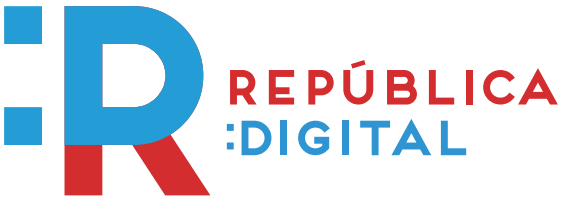
**IDS:** Un sistema de detección de intrusiones (o IDS de sus siglas en inglés Intrusion Detection System) es un programa de detección de accesos no autorizados a un computador o a una red.

**Host:** Un host o anfitrión es un ordenador que funciona como el punto de inicio y final de las transferencias de datos. Más comunmente descrito como el lugar donde reside un sitio web. El término host también se utiliza para referirse a una compañía que ofrece servicios de alojamiento para sitios web.

**Credssp:** El protocolo del proveedor de soporte de seguridad de credenciales ( CredSSP ) es un proveedor de soporte de seguridad que se implementa mediante la interfaz del proveedor de soporte de seguridad (SSPI).

**CVE:** Es una lista tipo diccionario de nombres estandarizados para vulnerabilidades y otra información relacionada con exposiciones de seguridad. CVE tiene como objetivo estandarizar los nombres de todas las vulnerabilidades y exposiciones de seguridad conocidas públicamente.

**Atacante:** El atacante es un individuo u organización que intenta obtener el control de un sistema informático para utilizarlo con fines maliciosos, robo de información vulnerabilidad.


REPÚBLICA
:DIGITAL