**Microsoft SQL Server Contraseña por defecto**

|  |
| --- |
| IP |
| 10.1.20.82 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/1433** | **Alta**  Alta / CVSS Base Score : 7.5 (CVSS2#AV:N AC:L/Au:N/C:P I:P/A:P) | La instancia de Microsoft SQL Server tiene establecida la cuenta 'sa' sin contraseña, esto puede permitir a un atacante acceder al manejador de base de datos con privilegios administrativos (dba) y acceder a los datos en las bases de datos y potencialmente ejecutar comandos sobre el sistema operativo. |
| Solución: | | |
| Filtrar el trafico entrante al puerto y establecer una contraseña para la cuenta 'sa' según la política de la organización a través del comando "osql -U sa" desde el sistema operativo, el store procedure "EXEC sp\_password" desde la consola SQL o por medio de la consola grafica. | | |

**MySQL < 3.23.59/4.0.21 Múltiples vulnerabilidades**

|  |
| --- |
| IP |
| 128.100.80.66 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/3306** | **Alta**  Alta / CVSS Base Score : 7.5  (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P) | El equipo remoto esta ejecutando una versión de la base de datos MySQL que es anterior que 4.0.21 o 3.23.59.  MySQL es una base de datos que se ejecuta en plataformas Linux/BSD y Windows.  La versión remota de este software es vulnerable a una consulta especialmente diseñado 'ALTER TABLE SQL', que puede ser explotada para evadir ciertas restricciones de seguridad aplicadas o causar una denegación de servicio (DoS).  Para aprovechar esta vulnerabilidad, un atacante tendría la capacidad de ejecutar sentencias arbitrarias de SQL en el equipo remoto. |
| Solución: | | |
| Actualizar MySQL a la versión 3.23.59 o 4.0.21 o a la más reciente.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**MySQL < 4.0.21 mysql\_real\_connect( desbordamiento)**

|  |
| --- |
| IP |
| 128.100.80.66 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/3306** | **Alta**  Alta / CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto está ejecutando una versión de MySQL anterior a 4.0.21.  MySQL es una base de datos que se ejecuta en los sistemas operativos Linux/BSD y Windows. Esta versión es vulnerable a un desbordamiento de longitud dentro de la función mysql\_real\_connect (). El desbordamiento se debe a un error en el procesamiento de un return Domain (DNS). Un ataque exitoso le daría al atacante la posibilidad de ejecutar código arbitrario en la máquina remota. |
| Solución: | | |
| Actualizar a la versión más reciente de MySQL  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**MySQL Zero-length Scrambled String Crafted Packet evasión de autenticación**

|  |
| --- |
| IP |
| 128.100.80.66 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/3306** | **Alta**  Alta / CVSS Base Score : 7.5  (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P) | Un error en la versión de MySQL que se esta ejecutando en el equipo remoto, puede permitirle a un atacante local evadir el mecanismo de autenticación utilizando un paquete especialmente diseñado con un zero-length scramble buff string.  Un atacante con el conocimiento de una cuenta existente definido para el servicio afectado puede aprovechar esta vulnerabilidad para evadir la autenticación y obtener acceso total a esa cuenta. |
| Solución: | | |
| Actualizar MySQL 4.1.3 o mas reciente  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Apache Tomcat Archivos de ejemplo**

|  |
| --- |
| **IP** |
| 10.1.20.76 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/9090** | **Media**  Medium / CVSS Base Score : 4.3  (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) | El sistema remoto expone archivos de ejemplos de JSPs y Servlets instalado en Apache Tomcat. |
| Solución: | | |
| Las mejores prácticas indican que un sistema en producción no debe exponer archivos de ejemplo o documentación, pues estos pueden proporcionar información útil a un atacante o pueden llegar a ser susceptibles a diversas vulnerabilidades. | | |

**Cadena de Certificados SSL cuenta con claves RSA débiles**

|  |
| --- |
| **IP** |
| 10.1.20.100 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/6767** | **Media**  Media / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) | Al menos uno de los certificados X.509 enviados por el equipo remoto tiene una clave que es más corta de 1024 bits. Estas claves se consideran débiles debido a los avances en la potencia para factorizar las claves criptográficas.  algunas implementaciones de SSL, en particular de Microsoft, puede considerar esta cadena SSL a ser válida debido a la longitud de una o más de las claves RSA que contiene. |
| Solución: | | |
| Vuelva a colocar el certificado de la cadena con la clave RSA débil con una llave fuerte.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Certificado Digital Expirado**

|  |
| --- |
| **IP** |
| 10.10.10.101 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/443** | **Media**  Media / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) | El certificado digital del servicio en el sistema remoto ha expirado o está a punto de expirar. |
| Solución: | | |
| Generar un nuevo certificado digital para el servicio. | | |

**Certificado Digital SSL con Nombre de equipo equivocado**

|  |
| --- |
| **IP** |
| 10.10.10.65 |
| 10.1.20.82 |
| 10.1.20.100 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/** **994**  **TCP/443**  **TCP/6767** | **Media**  Media / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) | El commonName (CN) del certificado SSL presentadno en este puerto es diferente al del equipo. |
| Solución: | | |
| Generar un nuevo certificado digital para el servicio. | | |

**Certificado SSL firmado por si mismo**

|  |
| --- |
| **IP** |
| 10.10.10.65 |
| 10.1.20.82 |
| 10.1.20.100 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/994**  **TCP/443**  **TCP/6767** | **Media**  Media / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) | El certificado X.509 para este servicio no se encuentra firmado por una autoridad certificadora autorizada. Si el equipo remoto es un equipo publico, esto nulificara la utilización del protocolo SSL para que pueda ser establecido con algún cliente, un atacante podría llevar a cabo un ataque del tipo man in the middle contra el equipo afectado. |
| Solución: | | |
| Comprar o generar un nuevo certificado para este servicio. | | |

**Certificado SSL firmado por una autoridad certificadora desconocida**

|  |  |  |  |
| --- | --- | --- | --- |
| **IP** | | | |
| 10.10.10.65 | 10.10.10.101 | 10.1.20.82 | 10.1.20.100 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/** **994**  **TCP/443**  **TCP/8834**  **TCP/1241**  **TCP/6767** | **Media**  Media / CVSS Base Score : 5.8  (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N) | El certificado X.509 de el cliente remoto no esta firmado por una autoridad certificadora publica conocida. Si el equipo remoto es un equipo publico en producción, este anula el uso de SSL y cualquiera puede establecer un ataque de hombre en medio contra el equipo remoto. |
| Solución: | | |
| Generar un certificado apropiado para este servicio | | |

**FTP Anónimo**

|  |
| --- |
| **IP** |
| 10.10.10.54 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/21** | **Media**  Media / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) | El servicio FTP en el sistema remoto permite acceso anónimo. |
| Solución: | | |
| Se recomienda que el acceso a archivos mediante sistemas remotos sea a través de un usuario y contraseña que delimite específicamente los permisos y privilegios del mismo, en caso de que el acceso publico sea correcto entonces validar que la información expuesta no es sensible y/o establecer un filtrado de IP's que puedan acceder al servicio. | | |

**Microsoft Windows Autenticación Nula en SMB**

|  |  |  |
| --- | --- | --- |
| **IP** | | |
| 128.100.80.66 | 10.10.10.97 | 10.1.20.76 |
| 128.100.80.33 | 10.10.10.65 | 10.1.20.68 |
| 128.100.80.29 | 10.10.10.54 | 10.1.20.103 |
| 128.100.80.158 | 10.1.20.82 | 10.1.20.100 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Media**  Media / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) | El equipo remoto permite acceder utilizando una sesión nula de SMB. Dependiendo de la configuración un atacante podría obtener información sobre el equipo remoto. |
| Solución: | | |
| Consultar las siguientes ligas para la solución  http://support.microsoft.com/kb/q143474/  http://support.microsoft.com/kb/q246261/ | | |

**MySQL < 4.0.21 mysqlhotcopy Creación temporal de un archivo inseguro**

|  |
| --- |
| **IP** |
| 128.100.80.66 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/3306** | **Media**  Media / CVSS Base Score : 4.6  (CVSS2#AV:L/AC:L/Au:N/C:P/I:P/A:P) | El equipo esta ejecutando una versión de MySQL anterior a 4.0.21  Mysqlhotcopy cuenta con una vulnerabilidad temporal inseguro debido a la creación de archivo. El resultado de esto es que los archivos temporales creados por la aplicación puede utilizar nombres de archivo predecibles.  Un atacante local podría aprovechar esta vulnerabilidad para ejecutar el archivo después de haber sobrescrito el contenido, Esta vulnerabilidad solo es local. |
| Solución: | | |
| Actualizar a la versión mas reciente de MySQL  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**MySQL Acceso a información sensible**

|  |
| --- |
| **IP** |
| 128.100.80.66 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/3306** | **Media**  Media / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) | El manejador de base de datos MySQL en el sistema remoto lee memoria no inicializada cuando procesa paquetes de login maliciosos. Un atacante puede aprovechar este problema para acceder a información sensible del sistema afectado. |
| Solución: | | |
| Actualizar a MySQL 4.0.27 / 4.1.22 / 5.0.86 / 5.1.40 o posterior. http://dev.mysql.com/downloads/  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Servidor FTP Genérico Directorios con permisos de escritura**

|  |
| --- |
| **IP** |
| 10.10.10.54 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/21** | **Media**  Media / CVSS Base Score : 6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) | El servidor FTP generic tiene directorios con permisos de escritura de forma global. |
| Solución: | | |
| Configurar el servicio de FTP para eliminar los permisos de escritura al resto de usuarios. | | |

**SMB: firma en la autenticación no habilitado**

|  |  |  |  |
| --- | --- | --- | --- |
| **IP** | | | |
| 192.168.1.32 | 128.100.80.29 | 10.10.10.54 | 10.1.20.68 |
| 128.100.80.79 | 128.100.80.158 | 10.10.10.101 | 10.1.20.103 |
| 128.100.80.66 | 10.10.10.97 | 10.1.20.82 | 10.1.20.100 |
| 128.100.80.33 | 10.10.10.65 | 10.1.20.76 | 10.10.10.72 |
| 10.10.10.50 | 10.1.20.87 | 10.1.20.75 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Media**  Media / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) | La firma en la autenticación se encuentra deshabilitada en el servidor remoto SMB. Esto puede permitir los ataques man-in-the-middle contra el servidor SMB. |
| Solución: | | |
| Habilitar la utilización del firmado en la autenticación. En Windows, esta se encuentra en la Directiva de seguridad local. En Samba, la configuración se denomina "firma del servidor. | | |

**SSL Protocolo de cifrado inseguro**

|  |
| --- |
| **IP** |
| 10.10.10.65 |
| 10.10.10.101 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/994**  **TCP/443** | **Media**  Media / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) | El servidor remoto acepta peticiones cifradas utilizando el protocolo SSL 2.0, el cual sufre de diversas deficiencias criptográficas y se encuentra en desuso. Un atacante podría aprovechar esto para realizar un ataque de hombre en medio. |
| Solución: | | |
| Deshabilitar el soporte para SSL 2.0 y utilizar SSL3.0 o TLS 1.0 en su lugar. En el archivo de configuración httpd.conf o ssl.conf según corresponda, establecer.  SSLProtocol -ALL +SSLv3 +TLSv1  SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:-LOW:-SSLv2:-EXP | | |

**Terminal Services nivel de cifrado medio o bajo**

|  |  |  |
| --- | --- | --- |
| **IP** | | |
| 128.100.80.66 | 10.10.10.65 | 10.1.20.103 |
| 128.100.80.33 | 10.10.10.54 | 10.1.20.100 |
| 128.100.80.29 | 10.1.20.82 | 10.10.10.72 |
| 128.100.80.158 | 10.1.20.76 | 10.1.20.87 |
| 10.10.10.97 | 10.1.20.68 | 10.1.20.75 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/3389** | **Media**  Media / CVSS Base Score : 4.3 (VSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) | El servicio remoto de Terminal Services no se encuentra configurado para la utilización de un cifrado fuerte.  Mediante la utilización de un cifrado débil con este tipo de servicio, es posible que un atacante pueda observar sus comunicaciones por ejemplo, tomar screenshoots, etcétera. |
| Solución: | | |
| Cambiar el nivel de cifrado RDP por alguno de los siguientes :  3. High  4. FIPS Compliant | | |

**Terminal Services No requiere Autenticación a nivel de red (NLA)**

|  |
| --- |
| **IP** |
| 10.10.10.72 |
| 10.10.10.50 |
| 10.1.20.87 |
| 10.1.20.75 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/3389** | **Media**  Media / CVSS Base Score : 4.3 (VSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) | El equipo remoto tiene el servicio de Terminal Services y no se encuentra configurado con la utilización del modulo de criptografía fuerte.  Utilizando criptografía débil en el servicio, el atacante podría interceptar las comunicaciones de manera mas fácil obteniendo capturas de pantalla y capturar la información del teclado. |
| Solución: | | |
| Habilitar Network Level Authentication (NLA) en el equipo remoto RDP. Esto generalmente se realiza en la pestaña 'Remote' en la configuración de Windows. | | |

**Terminal Services vulnerable a Man in The Midle (Ataque de hombre en medio)**

|  |  |  |
| --- | --- | --- |
| **IP** | | |
| 128.100.80.66 | 10.10.10.65 | 10.1.20.103 |
| 128.100.80.33 | 10.10.10.54 | 10.1.20.100 |
| 128.100.80.29 | 10.1.20.82 | 10.10.10.72 |
| 128.100.80.158 | 10.1.20.76 | 10.1.20.87 |
| 10.10.10.97 | 10.1.20.68 | 10.1.20.75 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/3389** | **Media**  Media / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) | El servicio Terminal Services en el host remoto es propenso a un ataque de hombre en medio y robo de sesión con lo cual un atacante podría obtener acceso al sistema con las credenciales del usuario conectado vía Terminal Service. |
| Solución: | | |
| Forzar el uso de SSL en las conexiones. Si no es posible crear un túnel de ssh para el uso del servicio. | | |

**Uso de llaves débiles para cifrado SSL**

|  |
| --- |
| **IP** |
| 10.1.20.100 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/6767** | **Media**  Media / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) | El sistema remoto soporta el uso de llaves SSL débiles (<=56bits) que ofrecen un cifrado débil para la comunicación de los datos. |
| Solución: | | |
| Reconfigure el sistema afectado para evitar el uso de llaves débiles, se recomienda que las llaves sean de 128bits o superiores. | | |

**El certificado digital SSL a sido firmado utilizando un algoritmo débil de hash (digestión)**

|  |
| --- |
| **IP** |
| 10.1.20.100 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/3389** | **Baja**  Baja / CVSS Base Score : 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N) | El sistema remoto utiliza un certificado digital SSL que a sido firmado utilizando una algoritmo de hash (digestión) débil como MD2, MD4, o MD5. Estos algoritmos son vulnerables a un ataque de colisión, lo que puede permitir a un atacante generar un certificado con el mismo hash (digestión) que el original y de esta manera suplantar identidades y captar trafico cifrado. |
| Solución: | | |
| Solicitar un nuevo certificado a la entidad certificadora correspondiente. | | |

**El servicio de Terminal Services no es FIPS-140 compliant**

|  |  |  |
| --- | --- | --- |
| **IP** | | |
| 128.100.80.66 | 10.10.10.65 | 10.1.20.103 |
| 128.100.80.33 | 10.10.10.54 | 10.1.20.100 |
| 128.100.80.29 | 10.1.20.82 | 10.10.10.72 |
| 128.100.80.158 | 10.1.20.76 | 10.1.20.87 |
| 10.10.10.97 | 10.1.20.68 | 10.1.20.75 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/3389** | **Baja**  Baja / CVSS Base Score : 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N) | El nivel de cifrado utilizado en el servicio de escritorio remoto no es FIPS-140 compliant. |
| Solución: | | |
| Establecer el nivel de cifrado del protocolo RDP a 4 "FIPS Compliant". | | |

**Renegociación de conexiones TLS / SSL**

|  |
| --- |
| **IP** |
| 10.1.20.100 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/23** | **Baja** | La implementación de los protocolos TLS y SSL utilizados por el servidor web, falla al asociar la renegociación de handshakes de una conexión preexistente, lo que puede permitir a un atacante realizar un ataque de hombre en medio (man-in-the-middle) para insertar datos en las sesiones HTTPS y posiblemente sustraer datos transmitidos en el canal seguro, al enviar una petición no autenticada que es procesadas retroactivamente por el servidor en una post renegociación del contexto de la conexión original, generando un ataque de inyección de texto plano "plaintext injection attack", comúnmente conocido como problema del "Project Mogul". |
| Solución: | | |
| Validar el uso del servicio, en caso de no ser necesario, consultar al fabricante sobre la des habilitación del Actualizar, el servidor web y las librerías relacionadas con SSL asociadas a la ultima versión disponible.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Servicio Telnet**

|  |
| --- |
| **IP** |
| 10.10.10.65 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/23** | **Baja** | El sistema remoto está ejecutando el servicio telnet. Este servicio es usado para la administración remota de equipos. La arquitectura de este servicio, lo hace inseguro ya que la comunicación en el cliente y el servidor se lleva a cabo sin ningún cifrado, esto lo hace propenso a ataques de robo de sesión, el cual permite tomar control total del sistema. |
| Solución: | | |
| Validar el uso del servicio, en caso de no ser necesario, consultar al fabricante sobre la des habilitación del servicio, si es requerido entonces establecer un filtrado para la conexión al puerto/servicio. | | |

**Soporte de envío de información en texto claro en Servicio FTP**

|  |
| --- |
| **IP** |
| 10.10.10.54 |
| 10.1.20.76 |
| 10.1.20.103 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/21** | **Baja** | El sistema remoto ejecuta el servicio de FTP, este servicio para transferencia de archivos transmite la información del usuario en texto claro, por lo que es posible interceptar las credenciales de accesos al servicio, así como los datos a través de un ataque de hombre en medio (MiTM) por medio de un sniffer en el segmento de red donde se produce la comunicación. |
| Solución: | | |
| Utilizar SFTP en lugar de este servicio o filtrar el trafico entrante al puerto o encapsular el trafico en un canal de SSL. | | |

**SSL RC4 Cipher Suites Supported**

|  |
| --- |
| **IP** |
| 10.10.10.54 |
| 10.1.20.76 |
| 10.1.20.103 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/** **994**  **TCP/443**  **TCP/8834**  **TCP/1241**  **TCP/6767** | **Baja** | El equipo remoto soporta el uso de RC4 en uno o mas suites de cifrado. El sistema de cifrado RC4 es defectuoso en su generación de una secuencia pseudo-aleatoria de bytes de modo que una amplia variedad de pequeños riesgos se introducen en la corriente, disminuyendo su aleatoriedad.  Si es texto plano repetidamente cifrado (por ejemplo, cookies HTTP), y un atacante puede obtener muchos textos cifrados (es decir, decenas de millones), el atacante puede ser capaz de obtener el texto en claro. |
| Solución: | | |
| Reconfigurar la aplicación afectada, si es posible, de evitar el uso del cifrado RC4. | | |