**7-Zip < 4.57 Problemas en el manejo de archivos**

|  |
| --- |
| IP |
| 99.41.24.220 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 9.3  (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)  (CVSS2#E:F/RL:OF/RC:C) | El equipo remoto contiene una versión del software de código libre 7-Zip el cual viene incluido con un software de un tercero llamado Turbo Searcher.  La versión de 7-Zip instalada en el equipo remoto se ve afectada por una vulnerabilidad no específica en el momento del manejo de los archivos. |
| Solución: | | |
| Actualizar a la versión 7Zip 4.57 o superior.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**ActiveX Conjunto de actualizaciones**

|  |
| --- |
| IP |
| 99.41.24.220 |
| 99.41.24.123 |
| 99.41.24.30 |
| 99.41.24.19 |
| 99.41.24.167 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 9.3  (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)  (CVSS2#E:F/RL:OF/RC:C) | Actualizar los controles ActiveX del host Windows remoto.Tenga en cuenta que los controles afectados son de otros fabricantes que han pedido a Microsoft a impedir que sus controles se ejecuten en Internet Explorer. Además uno o muchos controles de ActiveX Data Dynamics ActiveBar instalados en el equipo Windows se ven afectados por una vulnerabilidad de ejecución de código debido a problemas en los métodos: 'Save()', 'SaveLayoutChanges()', 'SaveMenuUsageData()', y en 'SetLayoutData()'. |
| Solución: | | |
| Se recomienda actualizar los controles ActiveX. Recordando que toda actualización puede tener impacto en los sistemas. Si la organización decide no instalar la actualización, esto debe de estar documentado.  Para más información, visite el siguiente enlace:  <http://support.microsoft.com/kb/2562937> | | |

**Adobe Photoshop CS5 < 12.0.4 Múltiples Vulnerabilidades no especificadas**

|  |
| --- |
| **IP** |
| 99.41.24.220 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alto / CVSS Base Score : 7.2  (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C) | La versión instalada de Adobe Photoshop CS5 es anterior a la 12.0.4, y por tanto es afectada a múltiples vulnerabilidades no especificadas. |
| Solución: | | |
| Aplicar la Actualizar Adobe Photoshop a la versión 12.0.4 o posterior.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**BlackBerry Desktop Software <6,0 B47 Subversión ruta DLL, permite la ejecución de código arbitrario e inyección**

|  |
| --- |
| **IP** |
| 99.41.24.220 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 7.2  (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C) | BlackBerry Desktop Software tiene una vulnerabilidad de la carga de DLL que se produce cuando el programa busca un archivo DLL en el directorio. Los atacantes pueden explotar el problema mediante la colocación de un archivo con extensión DLL especialmente diseñado y otros archivos asociados a la aplicación en un lugar controlado por el atacante. Cuando el archivo asociado se inicia, el código arbitrario del atacante puede ejecutarse. |
| Solución: | | |
| Actualizar a la versión BlackBerry Desktop Software 6.0 B47 o superior. | | |

**El agente de SNMP tiene configurada la comunidad "public"**

|  |
| --- |
| **IP** |
| 99.41.24.98 |
| 99.41.24.97 |
| 99.41.24.101 |
| 99.41.24.100 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **UDP/161** | **Alta**  Alta / CVSS Base Score : 7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C) | Es posible obtener el nombre de la comunidad por default: "public" esta configurada en el agente del protocolo SNMP. Un atacante remoto puede utilizar esta mala configuración para obtener información sensible del sistema afectado. |
| Solución: | | |
| Cambiar el nombre de la comunidad a una personalizada por el administrador del servicio, si es posible, configurar la versión 3 de SNMP, que incluye un mecanismo de cifrado para las respuestas del servicio.  Evaluar si el servicio no es necesario y en su defecto deshabilitarlo. | | |

**FlexNet Connect Múltiples vulnerabilidades de ejecución de código en el servicio de actualización**

|  |
| --- |
| **IP** |
| 99.41.24.220 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C) | La versión de FLEXnet Client Connect instalada en el equipo remoto incluye un control ActiveX - el "InstallShield Update Service Agent" - el cual está marcado como "seguro para scripting" y contiene varios métodos que permiten la descarga y el lanzamiento de programas arbitrarios. Si un atacante remoto logra engañar a un usuario de alguna máquina afectada para que visite una página web especialmente diseñada, podría de aprovechar este problema para ejecutar código arbitrario sujeto a los privilegios del usuario. |
| Solución: | | |
| Se recomienda ampliamente, instalar las actualizaciones correspondientes, recordando que toda actualización puede tener impacto en los sistemas. Si la organización decide no instalar la actualización, esto debe de estar documentado.  http://support.installshield.com/kb/view.asp?articleid=Q113602  <http://support.installshield.com/kb/view.asp?articleid=Q113020> | | |

**HP Data Protector ejecución de código remoto**

|  |
| --- |
| **IP** |
| 99.41.24.100 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/5555** | **Alta**  Alta / CVSS Base Score : 7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C) | El cliente remoto de HP Data Protector o el servicio del servidor afectado por una vulnerabilidad de ejecución de código. En donde un usuario con malas intenciones puede enviar un paquete especialmente diseñado, con el propósito de ejecutar código arbitrario en la shell con privilegios de root en caso de sistemas Unix y Linux y con privilegios de system en caso de Microsoft Windows. |
| Solución: | | |
| Actualizar Data Protector a la versión A.06.20 o posterior, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado.  Por otra parte, también se puede configurar el cliente al modo "secure" en el servicio CRS por lo que sólo puede originar comandos desde el servidor de CELL. Si este servicio no es necesario, debe estar desactivado. | | |

**Microsoft Office Service Pack desactualizado**

|  |
| --- |
| **IP** |
| 99.41.24.220 |
| 99.41.24.201 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C) | La versión de Microsoft Office no tiene service pack o el que tiene ya no es soportado actualmente. |
| Solución: | | |
| Instalar la última versión de service pack | | |

**Microsoft Silverlight versión NO Soportada (Windows)**

|  |
| --- |
| **IP** |
| 99.41.24.220 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  Alta / CVSS Base Score : 7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C) | De acuerdo a la versión, la instalación de Microsoft Silverlight en el equipo Microsoft Windows ya no es soportada. Como resultado de esto, esta aplicación contiene múltiples vulnerabilidades de seguridad. |
| Solución: | | |
| Actualizar a una versión de Microsoft Silverlight que se encuentre actualmente soportada.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Oracle Java SE | JDK | SDK | JRE Múltiples Vulnerabilidades**

|  |
| --- |
| **IP** |
| 99.41.24.123 |
| 99.41.24.128 |
| 99.41.24.131 |
| 99.41.24.167 |
| 99.41.24.19 |
| 99.41.24.220 |
| 99.41.24.30 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto contiene un entorno de ejecución que se ve afectado pormúltiples vulnerabilidades.  Descripción:  La versión de Oracle Java SE| JRE 6.x | JDK o Java for Business instalada en el equipo es menor a la versión 7 Update 3 / 6 Update 31 / 5.0 Update 34 / 1.4.2\_36, la cual se encuentra afectada por múltiples problemas de seguridad relacionados con los siguientes componentes:  - 2D  - AWT  - CORBA  - Concurrency  - Deployment  - I18n  - Install  - Java Runtime Environment  - Lightweight HTTP Server  - Serialization  - Sound  - Un error de stackoverflow relacionado con túneles. (Bug # 6670868)  - Existe un error en relación con las excepciones de seguridad en"AnnotationInvocationHandler.getMemberMethods.  (Bug # 6761678)  - Un error en 'URI.equals "puede permitir a un valor de retorno "verdadero" cuando se manejan octetos escapado. (Bug # 7041800)  - Un error relacionado con "LiveConnect" puede causar que las cookies no sean transferidas. (Bug # 7102914)  - La conectividad SSL se rompe cuando se utiliza el sistema de codificación TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA. (Bug # 7103725) |
| Solución: | | |
| Actualizar a JDK / JRE 7 Update 3 / 6 Update 31, JDK 5.0 Update 34, SDK 1.4.2\_36 o superior y remover las versiones necesarias del equipo afectado.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Trend Micro Antivirus**

|  |  |
| --- | --- |
| **IP** | |
| 99.41.24.220 | 99.41.24.220 |
| 99.41.24.128 | 99.41.24.128 |
| 99.41.24.123 | 99.41.24.123 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  Alta / CVSS Base Score : 9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C) | El antivirus Trend Micro, se instala en la máquina remota, pero este no funciona correctamente. |
| Solución: | | |
| Actualizar la aplicación y asociar los servicios que se estén ejecutando. | | |

**VLC Media Player < 1.1.9 presenta múltiples vulnerabilidades**

|  |
| --- |
| **IP** |
| 99.41.24.220 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C) | La versión de VLC media player instalado en la máquina remota es anterior a 1.1.9. Estas versiones n afectadas por múltiples vulnerabilidades:  - Un desbordamiento de búfer basado en heap existe en la función 'MP4\_ReadBox\_skcr' en modules/demux/mp4/libmp4.c.  Este problema se puede presentar cuando el análisis de un archivo MP4 con contenido malicioso, conduce que la aplicación se bloque y posiblemente la ejecución de código arbitrario. |
| Solución: | | |
| Actualizar VLC Media Player a la versión 1.1.9 o posterior. | | |

**HP Ignite-UX TFTP Divulgación de Información**

|  |
| --- |
| **IP** |
| 99.41.24.100 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **UDP/69** | **Media**  Media / CVSS Base Score : 4.3 (VSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) | El sistema remoto tiene activo un servicio de TFTP que comparte uno o varios archivos HP Ignite-UX, estos archivos pueden contener información sensible del sistema. |
| Solución: | | |
| Validar el uso de este servicio, si no es necesario entonces desactivarlo, de lo contrario restringir el acceso a fuentes confiables. | | |

**HP MFP Digital Sending Software < 4.18.3 Evasión de autenticación local**

|  |
| --- |
| **IP** |
| 99.41.24.220 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Media**  Media / CVSS Base Score : 4.3 (VSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) | El equipo remoto de Windows contiene una versión de HP MFP Digital Sending Software menor a la versión 4.18.3. Dicha versión se ve afectada por una vulnerabilidad de evasión de autenticación.  Un atacante local, podría explotar esta vulnerabilidad y obtener acceso no autorizado para poder enviar correos electrónicos y llevar a cabo otras funcionalidades de HP Multifunction Peripheral (MFP). |
| Solución: | | |
| Actualizar a HP MFP Digital Sending Software 4.18.5 o superior.  Nota: HP inicialmente recomienda actualizar a la versión 4.18.3, mientras que la versión que maneja esta vulnerabilidad introduce un defecto de seguridad por lo cual al final HP recomienda actualizar a la versión 4.18.5.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Microsoft Windows Autenticación Nula en SMB**

|  |
| --- |
| **IP** |
| 99.41.24.220 |
| 99.41.24.201 |
| 99.41.24.115 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Media**  Media / CVSS Base Score : 5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/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/ | | |

**REXECD se encuentra ejecutándose en el sistema remoto**

|  |
| --- |
| **IP** |
| 99.41.24.100 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/512** | **Media**  Media / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) | El sistema remoto esta ejecutando el servicio rexecd. 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 acabo sin ningún cifrado, esto los hace propenso a ataques de robo de sesión, el cual permite tomar control total del sistema. |
| Solución: | | |
| Validar el uso del servicio. Si el servicio no es requerido, consultar la documentación del fabricante sobre la desactivación del servicio. Si es requerido entonces establecer un filtrado para la conexión al puerto/servicio. | | |

**Rlogin se encuentra ejecutándose en un sistema remoto**

|  |
| --- |
| **IP** |
| 99.41.24.100 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/513** | **Media**  Media / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) | El sistema remoto esta ejecutando el servicio rlogin. 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 acabo sin ningún cifrado, esto los hace propenso a ataques de robo de sesión, el cual permite tomar control total del sistema. |
| Solución: | | |
| Validar el uso del servicio. Si el servicio no es requerido, consultar la documentación del fabricante sobre la desactivación del servicio. Si es requerido entonces establecer un filtrado para la conexión al puerto/servicio. | | |

**SMTP Enumeración de nombres de usuarios y grupos**

|  |
| --- |
| **IP** |
| 99.41.24.100 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/25** | **Media**  Media / CVSS Base Score : 4.3 (VSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) | El servidor de SMTP en el sistema remoto responde comandos EXPN y/o VRFY, estos comandos pueden ser utilizados para encontrar cuentas, nombres completos y alias de las cuentas en el servidor |
| Solución: | | |
| Deshabilitar el acceso a estos comandos para usuarios remotos agregando la opción:  O PrivacyOptions=goaway en el archivo de configuración de Sendmail /etc/sendmail.cf o equivalente. | | |

**SSH Protocolo de cifrado inseguro**

|  |
| --- |
| **IP** |
| 99.41.24.97 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/22** | **Media**  Media / CVSS Base Score : 4.3 (VSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) | El servicio SSH en el sistema remoto acepta peticiones cifradas utilizando el protocolo SSH 1.33 y/o 1.5, 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 protocolo SSH 1.X y utilizar SSH 2.0 en su lugar. | | |

**SSL Protocolo de cifrado inseguro**

|  |
| --- |
| **IP** |
| 99.41.24.201 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/8443** | **Media**  Media / CVSS Base Score : 4.3 (VSS2#AV:N/AC:M/Au:N/C:N/I:P/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 | | |

**Sun Java JRE Problemas de denegación de servicio en la librería dinámica jpiexp32.dll**

|  |
| --- |
| **IP** |
| 99.41.24.220 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Media**  Media / CVSS Base Score : 4.3 (VSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) | De acuerdo con su número de versión de Sun Java Runtime Environment (JRE) instalado en el equipo remoto, contiene un tema en 'jpiexp32.dll' que pueden dar lugar a una excepción de puntero nulo cuando una referencia a objetos HTML de un applet de Java, pero no define el atributo 'name'. Si un atacante remoto puede engañar a un usuario en la máquina afectada para que visite una página web especialmente diseñado, que puede ser capaz de aprovechar este problema para hacer que el JRE e Internet Explorer deje de funcionar. |
| Solución: | | |
| Actualizar Sun Java 2 JDK y JRE 5.0 update 14 o posterior.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Sun Java Web Start JNLP problemas de desbordamiento de búfer**

|  |
| --- |
| **IP** |
| 99.41.24.220 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Media**  Media / CVSS Base Score : 4.3 (VSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) | Se informa, de un desbordamiento de búfer en la utilidad de Java Web Start distribuido con la versión de Sun Java Runtime Environment (JRE) instalado en la máquina remota. Si un atacante logra convencer a un usuario de la máquina afectada para abrir un archivo JNLP especialmente diseñado, puede ser capaz de ejecutar código arbitrario sujeto a los privilegios del usuario. |
| Solución: | | |
| Actualizar Sun Java JDK y JRE 6 Update 2 / JDK y JRE 5.0 Update 12 o posterior y remover si es necesario las versiones afectadas.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Terminal Services Vulnerable a Man in TheMidle (Ataque de hombre en medio)**

|  |  |
| --- | --- |
| **IP** | |
| 99.41.24.220 | 99.41.24.120 |
| 99.41.24.201 | 99.41.24.189 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/3389** | **Media**  Media / CVSS Base Score : 5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P) | 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** |
| 99.41.24.201 |

|  |  |  |
| --- | --- | --- |
| **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 sistema remoto soporta el uso de llaves SSL débiles (56bits >= 112bits) que ofrecen un cifrado débil para la comunicación de los datos. |
| 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 | | |

**Almacenamiento de credenciales en memoria**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **IP** | | | | |
| 99.41.24.131 | 99.41.24.122 | 99.41.24.115 | 99.41.24.220 | 99.41.24.201 |
| 99.41.24.128 | 99.41.24.123 | 99.41.24.30 | 99.41.24.19 | 99.41.24.167 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Baja**  Baja / CVSS Base Score : 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N) | La llave de registro \nHKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount\nis está establecida con un valor diferente a 0, esto significa que el sistema remoto almacena locamente las contraseñas en cache para permitir el acceso automático de los usuario en caso de una falla del PDC. |
| Solución: | | |
| Establecer el valor de la llave de registro a 0 | | |

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

|  |  |  |
| --- | --- | --- |
| **IP** | | |
| 99.41.24.220 | 99.41.24.201 | 99.41.24.189 |
| 99.41.24.120 |

|  |  |  |
| --- | --- | --- |
| **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". | | |

**Servicio Telnet**

|  |
| --- |
| **IP** |
| 99.41.24.98 |
| 99.41.24.97 |
| 99.41.24.101 |

|  |  |  |
| --- | --- | --- |
| **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. | | |

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

|  |
| --- |
| **IP** |
| 99.41.24.201 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/443** | **Baja** | 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. | | |

**Renegociación de conexiones TLS / SSL**

|  |
| --- |
| **IP** |
| 99.41.24.201 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/8443** | **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: | | |
| 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. | | |

**BlackBerry Desktop Software < 6.0.1 presenta vulnerabilidad en los archivos de respaldo, propensos ataques de fuerza bruta**

|  |
| --- |
| **IP** |
| 99.41.24.220 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Baja** | La versión de BlackBerry Desktop instalada en el equipo remoto es inferior a la versión 6.0.1. Dichas versiones utilizan una encriptación débil de contraseña para encriptar los archivos de respaldo, lo cual hace posible a un usuario local poder desencriptar lo archivos de respaldo a través de un ataque de fuerza bruta. |
| Solución: | | |
| Actualizar a BlackBerry Desktop Software 6.0.1 o superior. | | |

**Cisco Router Vulnerabilidad en la Solicitud SNMP que permite la divulgación de información**

|  |
| --- |
| **IP** |
| 99.41.24.98 |
| 99.41.24.97 |
| 99.41.24.101 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **UDP/161** | **Baja** | Es posible determinar el modelo de equipo remoto CISCO mediante el envío de peticiones SNMP con el OID 1.3.6.1.4.1.9.1.  Un atacante puede utilizar esta información para obtener más información sobre la máquina remota. |
| Solución: | | |
| Deshabilitar el servicio SNMP en el equipo remoto solo si no es utilizado o filtrar paquetes entrantes a este puerto. | | |