**ActiveX Conjunto de actualizaciones**

|  |
| --- |
| IP |
| 99.40.20.60 |
| 99.40.20.225 |

|  |  |  |
| --- | --- | --- |
| **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. |
| 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 Acrobat Reader < 10.1.3 / 9.5.1 Múltiples Vulnerabilidades (APSB12-08)**

|  |
| --- |
| IP |
| 99.40.20.230 |
| 99.40.20.60 |

|  |  |  |
| --- | --- | --- |
| **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) | La versión de Adobe Reader instalada en el equipo remoto es menor a la versión 10.1.3 / 9.5.1, estas versiones se ven afectadas por múltiples vulnerabilidades:  - Un desbordamiento de enteros existe en las fuentes de letras True Type Font (TFF). (CVE-2012-0774)  - Una vulnerabilidad de corrupción de memoria existe en el manejador de JavaScript. (CVE-2012-0775)  - Un problema de seguridad existe en Adobe Reader installer el cual podría ocasionar la evasión a ciertas restricciones de seguridad.  (CVE-2012-0776) |
| Solución: | | |
| Actualizar a Adobe Reader 9.5.1 / 10.1.3 o superior.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Adobe Flash Player <= 10.3.183.7 Múltiples Vulnerabilidades (APSB11-26)**

|  |
| --- |
| **IP** |
| 99.40.20.225 |
| 99.40.20.230 |
| 99.40.20.248 |
| 99.40.20.249 |
| 99.40.20.60 |
| 99.40.20.61 |
| 99.40.20.63 |
| 99.40.20.77 |

|  |  |  |
| --- | --- | --- |
| **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 Flash Player instalada en el equipo remoto es la 10.3.183.7 o anterior. Por lo tanto ha sido reportada como vulnerable a diversas vulnerabilidades críticas:    - Ejecución de código debido a desbordamientos de memoría en la pila (StackOverflow) (CVE-2011-2426, CVE-2011-2427)    - Ejecución de código o lograr que el navegador deje de responder debido a un error de lógica. (CVE-2011-2428)    - Revelación de información al evadir un control de seguridad de Flash Player (CVE-2011-2429)    - Ejecución de código en la lógica de reproducción de multimedia (CVE-2011-2430)    - Cross Site Scripting permite a un atacante realizar acciones en nombre del usuario que sea engañado para visitar un sitio web malicioso. (CVE-2011-2444) |
| Solución: | | |
| Actualizar Adobe Flash a la versión 10.3.183.10 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. | | |

**Adobe Shockwave Player 11.5.8.612 presenta múltiples vulnerabilidades**

|  |
| --- |
| **IP** |
| 99.40.20.77 |

|  |  |  |
| --- | --- | --- |
| **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 de Adobe Shockwave Player es anterior a la 11.5.8.612. Dichas versiones están afectadas por los siguientes problemas:  - Múltiples problemas de corrupción de memoria que podrían terminar en ejecución de código arbitrario.  - Una vulnerabilidad de puntero flotante permitiría la ejecución de código.  - Una vulnerabilidad de desbordamiento de entero permitiría la ejecución de código arbitrario. |
| Solución: | | |
| Actualizar a Adobe Shockwave 11.5.8.612 o posterior. Se recomienda visitar el siguiente enlace: http://www.symantec.com/avcenter/security/Content/2008.10.20a.html (Diríjase a la sección Symantec Response)  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Altiris AClient < 6.9.164 Múltiples Vulnerabilidades locales**

|  |
| --- |
| **IP** |
| 99.40.20.230 |
| 99.40.20.248 |
| 99.40.20.249 |
| 99.40.20.61 |
| 99.40.20.63 |

|  |  |  |
| --- | --- | --- |
| **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) | La versión del Agente de Altiris Client (aclient) instalado en el equipo remoto, es susceptible a un ataque que podría permitir a un usuario local elevar sus privilegios en los sistemas afectados. |
| Solución: | | |
| Actualizar Altiris Deployment Solution Agent a 6.9.164 o posterior. 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.  Se recomienda visitar el siguiente enlace: http://www.symantec.com/avcenter/security/Content/2008.10.20a.html Diríjase a la sección Symantec Response.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Altiris Deployment Solution Agent < 6.9.355 elevación de privilegios localmente (SYM08-019)**

|  |
| --- |
| **IP** |
| 99.40.20.230 |
| 99.40.20.248 |
| 99.40.20.249 |
| 99.40.20.61 |
| 99.40.20.63 |

|  |  |  |
| --- | --- | --- |
| **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) | La versión instalada de Altiris Deployment Solution Agent en el equipo remoto es afectada por un problema de elevación de privilegios. La explotación exitosa de este problema le puede permitir a usuarios no autorizados obtener acceso al equipo con privilegios de sistema local. |
| Solución: | | |
| Actualizar Altiris Deployment Solution 6.9 build 355 o posterior y actualizar los Agents.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**iTunes < 10.6.3 Múltiples Vulnerabilidades (credentialed check)**

|  |
| --- |
| **IP** |
| 99.40.20.249 |

|  |  |  |
| --- | --- | --- |
| **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 iTunes instalada en el equipo remoto Windows, es menor a la versión 10.6.3 y por lo tanto, se ve afectada por múltiples problemas de seguridad :  - Problemas de corrupción de memoria existen en el WebKit que podría permitir a sitios maliciosos corromper la aplicación y también ejecutar código arbitrario. (CVE-2012-0672)  - Problemas de Stack y heap buffer overflow relacionados con el manejo de listas de archivos 'm3u'. Podría ocacionar que la aplicación deje de responder o la ejecución de código arbitrario de forma remota (CVE-2012-0677) |
| Solución: | | |
| Actualizar a iTunes 10.6.3 o superior.  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** |
| 99.40.20.225 |
| 99.40.20.230 |
| 99.40.20.249 |
| 99.40.20.60 |
| 99.40.20.61 |
| 99.40.20.63 |
| 99.40.20.77 |

|  |  |  |
| --- | --- | --- |
| **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 por múltiples 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 stack overflow 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. | | |

### QuickTime < 7.7.2 Múltiples Vulnerabilidades

|  |
| --- |
| **IP** |
| 99.40.20.249 |

|  |  |  |
| --- | --- | --- |
| **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 QuickTime instalada en el equipo remoto Windows es menor a la versión 7.7.2, que se ve afectada por varios problemas de seguridad:  - Problemas de acceso a memoria no inicializada en el manejo de archivos codificados en MP4. (CVE-2011-3458)  - Desbordamiento de búfer en el manejo de archivos de peliculas en QuickTime. (CVE-2011-3459) (CVE-2012-0659) (CVE-2012-0660) (CVE-2012-0661) (CVE-2012-0663) (CVE-2012-0664) (CVE-2012-0665) (CVE-2012-0666) (CVE-2012-0667) (CVE-2012-0669)(CVE-2012-0670) (CVE-2012-0671) |
| Solución: | | |
| Actualizar QuickTime a la versión7.7.2 o superior.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Shockwave Player <= 11.6.1.629 cuenta con múltiples vulnerabilidades de corrupción de memoria (APSB11-27)**

|  |
| --- |
| **IP** |
| 99.40.20.77 |

|  |  |  |
| --- | --- | --- |
| **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 equipo remoto de Windows contiene una versión de Adobe Shockwave Player 11.6.1.629 o anterior. Que podría verse afectada por múltiples vulnerabilidades de corrupción de memoria.  Un atacante remoto podría explotar este error al lograr engañar a un usuario para que que visialice un archivo Shockwave malicioso, resultando en la ejecución de código arbitrario. |
| Solución: | | |
| Actualizar Adobe Shockwave 11.6.3.633 o superior. Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**VLC Media Player < 2.0.2 Múltiples vulnerabilidades**

|  |
| --- |
| **IP** |
| 99.40.20.248 |

|  |  |  |
| --- | --- | --- |
| **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) | La versión de VLC media player instalada en el equipo remoto es menor a la versión 2.0.2. Se ve afectada por diversos problemas de seguridad relacionados con problemas de heap-based buffer overflow.  Un error existe en la función 'Ogg\_DecodePacket' en el archivo 'modules/demux/ogg.c' el cual no valida de forma correcta la entrada lo cual podría ocasionar un heap-based buffer overflow, permitiendo la ejecución de código arbitrario. |
| Solución: | | |
| Actualizar a VLC Media Player 2.0.2 o superior. Alternativamente, se pueden remover los plugins que se ven afectados en el directorio de plugins de VLC's  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Winamp < 5.63 Múltiples vulnerabilidades**

|  |
| --- |
| **IP** |
| 99.40.20.61 |

|  |  |  |
| --- | --- | --- |
| **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 equipo remoto se encuentra ejecutando una versión de Winamp para Windows, esta versión se ve afectada por múltiples problemas de seguridad:  - Un problema de corrupción de memoria existe en 'in\_mod.dll' relacionado con una mala validación en el manejo de los archivos 'Impulse Tracker'.  - Diversos problemas de Heap-based buffer overflows existen en 'bmp.w5s' cuando se manejan datos de 'BI\_RGB' y 'UYVY' de archivos AVI.c  La explotación exitosa de este problema podría ocasionar la ejecución de código arbitrario en el equipo vulnerable. |
| Solución: | | |
| Actualizar a Winamp 5.63 (5.6.3.3234) o superior.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Windows Service Pack fuera de tiempo**

|  |
| --- |
| **IP** |
| 99.40.20.225 |
| 99.40.20.60 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  Alta / CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El sistema remoto no cuenta con la versión actualizada de Service Pack o la instalada no se admite en el equipo. |
| Solución: | | |
| Instalar la última versión de Service Pack | | |

**Adobe Flash Player < 10.3.181.22 Múltiples vulnerabilidades**

|  |
| --- |
| **IP** |
| 99.40.20.225 |
| 99.40.20.230 |
| 99.40.20.248 |
| 99.40.20.249 |
| 99.40.20.60 |
| 99.40.20.61 |
| 99.40.20.63 |
| 99.40.20.77 |

|  |  |  |
| --- | --- | --- |
| **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) | Una vulnerabilidad de cross-site scripting existe en versiones de Flash Player menores a 10.3.181.22 (10.3.181.23 para ActiveX).  Un atacante podría aprovechar este problema para inyectar y ejecutar código arbitrario HTML y código script en el navegador del usuario. |
| Solución: | | |
| Actualizar a la versión más reciente de Adobe Flash 10.3.181.22 (10.3.181.23 en ActiveX) 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. | | |

**Citrix XenApp Online Plug-in / Vulnerabilidad de suplantación de identidad (MiTM) a través de certificados especialmente diseñados**

|  |
| --- |
| **IP** |
| 99.40.20.230 |
| 99.40.20.248 |
| 99.40.20.249 |
| 99.40.20.61 |
| 99.40.20.63 |
| 99.40.20.77 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Media / CVSS Base Score : 5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N) | La versión instalada de Citrix Online Plug-in o ICA Client, en el equipo remoto cuenta con una vulnerabilidad puede ser aprovechada a través de un ataque de hombre en medio (Man in The Middle). Este problema esta reportado en el boletín MS09-056 de seguridad de Microsoft , y probablemente se deba a una falla en la detección de bytes nulos en el nombre común de un certificado. Un atacante remoto puede aprovechar esto para ejecutar un ataque "man-in-the-middle" y lograr leer o modificar el trafico de SSL/TLS al ser enviado desde el sistema. |
| Solución: | | |
| Actualizar Citrix Online Plug-in o Citrix ICA Client a la versión 11.0.150/11.2.0 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. | | |

**iTunes < 10.5.1 vulnerabilidad en la verificación de la autenticidad de actualizaciones**

|  |
| --- |
| **IP** |
| 99.40.20.249 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Media**  Media / CVSS Base Score : 5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P) | La versión instalada de iTunes en el equipo remoto Mac OS X es anterior a la 10.5.1. Como tal, utiliza una conexión HTTP insegura, al momento de revisar o descargar actualizaciones de software, que podría permitir a un atacante subir un troyano que paresca proveniente de Apple a través de un ataque de hombre-en-medio |
| Solución: | | |
| Actualizar iTunes a la versión 10.5.1 o superior. 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 JRE Problemas de denegación de servicio en la librería dinámica jpiexp32.dll**

|  |
| --- |
| **IP** |
| 99.40.20.225 |
| 99.40.20.60 |

|  |  |  |
| --- | --- | --- |
| **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** |
| 99.40.20.225 |
| 99.40.20.60 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Media**  Media / CVSS Base Score : 6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P) | 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. | | |

**Macrovision SafeDisc Desbordamiento de memoria local**

|  |
| --- |
| **IP** |
| 99.40.20.225 |
| 99.40.20.60 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Media**  Media / CVSS Base Score : 6.9 (CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C) | Macrovision SafeDisc, es una aplicación contra la generación de copias de cd/dvd para Microsoft Windows.  El controlador 'SECDRV.SYS' incluido con la versión de SafeDisc instalada en el equipo remoto, permite a un usuario local ganar privilegios de System, utilizando un argumento especialmente diseñado y mandándolo al método METHOD\_NEITHER IOCTL. |
| Solución: | | |
| Actualizar el controlador de Macrovision SECDRV.SYS a la versión 4.3.86 o posterior. | | |

**Microsoft Windows Autenticación Nula en SMB**

|  |
| --- |
| **IP** |
| 99.40.20.225 |
| 99.40.20.60 |

|  |  |  |
| --- | --- | --- |
| **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/ | | |

**Symantec pcAnywhere vulnerabilidad en archivos CHF podría permitir una denegación de servicio**

|  |
| --- |
| **IP** |
| 99.40.20.230 |
| 99.40.20.248 |
| 99.40.20.249 |
| 99.40.20.61 |
| 99.40.20.63 |
| 99.40.20.77 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Media**  Media / CVSS Base Score : 4.6 (CVSS2#AV:L/AC:L/Au:N/C:P/I:P/A:P) | La versión instalada de Symantec pcAnywhere en el equipo remoto de Windows no maneja apropiadamente el formato de cadena dentro de los nombres de archivos de control remotos (.CHF) o sus rutas de archivos asociadas. Utilizando un archivo especialmente diseñado o el nombre de la ruta, un usuario local puede explotar este problema con el propósito de leer o escribir en la memoria y como mínimo lograr que la aplicación afectada deje de funcionar. |
| Solución: | | |
| Actualizar pcAnywhere a la versión 12.5.0 Build 442 (también conocido como 12.5 SP1) 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. | | |

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

|  |
| --- |
| **IP** |
| 99.40.20.138 |
| 99.40.20.199 |
| 99.40.20.230 |
| 99.40.20.253 |
| 99.40.20.61 |
| 99.40.20.76 |

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

**Almacenamiento de credenciales en memoria**

|  |
| --- |
| **IP** |
| 99.40.20.225 |
| 99.40.20.230 |
| 99.40.20.248 |
| 99.40.20.249 |
| 99.40.20.60 |
| 99.40.20.61 |
| 99.40.20.63 |
| 99.40.20.77 |

|  |  |  |
| --- | --- | --- |
| **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** |
| 99.40.20.76 |
| 99.40.20.61 |
| 99.40.20.253 |
| 99.40.20.230 |
| 99.40.20.199 |
| 99.40.20.138 |

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

**Nessus UDP scanner**

|  |
| --- |
| **IP** |
| 99.40.20.199 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **UDP/General** | **Baja** | Es posible conocer los puertos y servicios que tiene habilitado el host mediante un escaneo de puertos UDP |
| Solución: | | |
| Aplicar reglas en el firewall para no permitir escaneos de tipo UDP | | |