**ActiveX Conjunto de actualizaciones**

|  |
| --- |
| IP |
| 99.40.40.236 |

|  |  |  |
| --- | --- | --- |
| **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 Múltiples Vulnerabilidades (APSB12-01)**

|  |  |
| --- | --- |
| IP | |
| 99.40.40.79 | 99.40.40.244 |
| 99.40.40.236 | 99.40.40.223 |
| 99.40.40.184 | 99.40.40.181 |
| 99.40.40.176 | 99.40.40.172 |
| 99.40.40.170 | 99.40.40.153 |
| 99.40.40.149 |

|  |  |  |
| --- | --- | --- |
| **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 instalada de Adobe Reader el equipo remoto es menor a la versión 10.1.2 / 9.5, además se ve afectada por múltiples vulnerabilidades relacionadas con la corrupción de memoria. Un atacante al explotar esta vulnerabilidad de forma exitosa, podría ejecutar código arbitrario de forma remota. |
| Solución: | | |
| Actualizar a Adobe Reader 9.5 / 10.1.2 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. | | |

**Adobe Flash Player <= 10.3.183.19 / 11.3.300.256 Múltiples Vulnerabilidades (APSB12-14)**

|  |  |  |
| --- | --- | --- |
| **IP** | | |
| 99.40.40.79 | 99.40.40.244 | 99.40.40.236 |
| 99.40.40.223 | 99.40.40.191 | 99.40.40.184 |
| 99.40.40.182 | 99.40.40.181 | 99.40.40.172 |
| 99.40.40.170 | 99.40.40.154 | 99.40.40.153 |
| 99.40.40.152 | 99.40.40.149 | 99.40.40.141 |
| 99.40.40.133 | 99.40.40.130 |

|  |  |  |
| --- | --- | --- |
| **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) | De acuerdo a la versión de Flash Player instalada en el equipo remoto, esta es la 10.x anterior a la 10.3.183.16 o 11.x igual o anterior a la 11.1.102.63. Por lo tanto es afectada por diversas vulnerabilidades de corrupción de memoria:  - Corrupción de vulnerabilidades relacionada al dominio de seguridad de URL. (CVE-2012-0772)  - Una falla en la clase NetStream podría resultar en ejecución de código (CVE-2012-0073)  - Dos vulnerabilidades de corrupción de memoria relacionadas a la interface de Google Chrome (CVE-2012-0724, CVE-2012-0725)  A través de engañar a un usuario para que visite un página especialmente diseñada, un atacante podría utilizar estas vulnerabilidades para ejecutar código sujeto a los privilegios del usuario. |
| Solución: | | |
| Actualizar Adobe Flash a la versión 11.2.202.228 / 10.3.183.20 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. | | |

**Altiris AClient < 6.9.164: Múltiples Vulnerabilidades locales**

|  |  |  |
| --- | --- | --- |
| **IP** | | |
| 99.40.40.79 | 99.40.40.244 | 99.40.40.236 |
| 99.40.40.223 | 99.40.40.191 | 99.40.40.184 |
| 99.40.40.182 | 99.40.40.181 | 99.40.40.176 |
| 99.40.40.172 | 99.40.40.170 | 99.40.40.154 |
| 99.40.40.153 | 99.40.40.152 | 99.40.40.149 |
| 99.40.40.141 | 99.40.40.133 | 99.40.40.130 |

|  |  |  |
| --- | --- | --- |
| **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 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 superior. 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) | | |

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

|  |  |  |
| --- | --- | --- |
| **IP** | | |
| 99.40.40.79 | 99.40.40.244 | 99.40.40.223 |
| 99.40.40.191 | 99.40.40.184 | 99.40.40.182 |
| 99.40.40.181 | 99.40.40.176 | 99.40.40.172 |
| 99.40.40.170 | 99.40.40.154 | 99.40.40.153 |
| 99.40.40.152 | 99.40.40.149 | 99.40.40.141 |
| 99.40.40.133 | 99.40.40.130 |

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

**El servicio VNC no requiere autenticación**

|  |
| --- |
| **IP** |
| 99.40.40.170 |

|  |  |  |
| --- | --- | --- |
| **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) | El servidor VNC en el sistema remoto permite conexión sin la necesidad de autenticación al servicio, esto puede permitir a un atacante visualizar la actividad de los usuarios y potencialmente tomar control del sistema afectado. |
| Solución: | | |
| Establecer una contraseña para el servicio y deshabilitar la opción de 'No Authentication'. | | |

**Microsoft .NET Framework Service Pack fuera de tiempo**

|  |
| --- |
| **IP** |
| 99.40.40.172 |

|  |  |  |
| --- | --- | --- |
| **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) | El sistema remoto tiene instalado Microsoft .NET Framework. La versión instalada no posee los service pack instalados, y si los tiene están desactualizados. |
| Solución: | | |
| Instalar la ultimo versión de service pack de Microsoft .NET Framework. | | |

**Microsoft Windows Update necesita ser reiniciado**

|  |
| --- |
| **IP** |
| 99.40.40.176 |
| 99.40.40.153 |
| 99.40.40.133 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 7.1 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:C) | De acuerdo con las entradas en el registro, es necesario reiniciar Windows Update para completar la instalación de al menos una actualización. Si los cambios pendientes están relacionados con la seguridad, el equipo remoto podría seguir siendo vulnerable a los ataques hasta que se produce un reinicio. |
| Solución: | | |
| Reiniciar el equipo afectado. | | |

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

|  |  |  |
| --- | --- | --- |
| **IP** | | |
| 99.40.40.79 | 99.40.40.244 | 99.40.40.236 |
| 99.40.40.223 | 99.40.40.191 | 99.40.40.184 |
| 99.40.40.182 | 99.40.40.181 | 99.40.40.176 |
| 99.40.40.172 | 99.40.40.170 | 99.40.40.154 |
| 99.40.40.153 | 99.40.40.152 | 99.40.40.149 |
| 99.40.40.141 | 99.40.40.133 | 99.40.40.130 |

|  |  |  |
| --- | --- | --- |
| **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) | Deacuerdo 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 (Jun 2012 CPU)**

|  |  |  |
| --- | --- | --- |
| **IP** | | |
| 99.40.40.79 | 99.40.40.244 | 99.40.40.223 |
| 99.40.40.191 | 99.40.40.184 | 99.40.40.182 |
| 99.40.40.181 | 99.40.40.176 | 99.40.40.172 |
| 99.40.40.170 | 99.40.40.154 | 99.40.40.153 |
| 99.40.40.152 | 99.40.40.149 | 99.40.40.141 |
| 99.40.40.133 | 99.40.40.130 |

|  |  |  |
| --- | --- | --- |
| **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) (CVSS2#E:F/RL:OF/RC: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. | | |

**Microsoft Windows Update necesita ser reiniciado**

|  |
| --- |
| **IP** |
| 99.40.40.176 |
| 99.40.40.153 |
| 99.40.40.133 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 7.1 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:C) | De acuerdo con las entradas en el registro, es necesario reiniciar Windows Update para completar la instalación de al menos una actualización. Si los cambios pendientes están relacionados con la seguridad, el equipo remoto podría seguir siendo vulnerable a los ataques hasta que se produce un reinicio. |
| Solución: | | |
| Reiniciar el equipo afectado. | | |

**QuickTime < 7.7.2 Múltiples Vulnerabilidades**

|  |  |  |
| --- | --- | --- |
| **IP** | | |
| 99.40.40.223 | 99.40.40.184 | 99.40.40.176 |
| 99.40.40.154 | 99.40.40.152 | 99.40.40.149 |
| 99.40.40.141 | 99.40.40.133 | 99.40.40.130 |

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

**QuickTime < 7.7.2 Múltiples Vulnerabilidades**

|  |  |  |
| --- | --- | --- |
| **IP** | | |
| 99.40.40.223 | 99.40.40.184 | 99.40.40.176 |
| 99.40.40.154 | 99.40.40.152 | 99.40.40.149 |
| 99.40.40.141 | 99.40.40.133 | 99.40.40.130 |

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

**QuickTime < 7.7.2 Múltiples Vulnerabilidades**

|  |  |  |
| --- | --- | --- |
| **IP** | | |
| 99.40.40.223 | 99.40.40.184 | 99.40.40.176 |
| 99.40.40.154 | 99.40.40.152 | 99.40.40.149 |
| 99.40.40.141 | 99.40.40.133 | 99.40.40.130 |

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

**RealVNC VNC Viewer < 4.1.3/4.4.3 Vulnerabilidad que podría permitir la ejecución de código arbitrario**

|  |
| --- |
| **IP** |
| 99.40.40.170 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 7.1 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:C) | La versión de RealVNC's VNC Viewer instalada en el equipo remoto Windows se ve afectada por múltiples vulnerabilidades:  - Un error en la función 'CMsgReader::readRect()' 'common/rfb/CMsgReader.cxx' que sucede cuando se ejecuta un archivo y se empiezan a decodificar ciertos tipos de archivos, lo cual ocasionaria la ejecución de código arbitrario en el equipo afectado.  - Mediante el engaño a un usuario un usuario se podría conectar a un servidor VNC malicioso y asi el atacante podría ejecutar código remoto en el sistema afectado al enviar datos mediante el protocolo RFB al componente VNC Viewer. El servidor VNC no se ve afectada por esta vulnerabilidad. |
| Solución: | | |
| Actualizar a RealVNC VNC Viewer Free Edition 4.1.3 / Personal Edition 4.4.3 / Enterprise Edition 4.4.3 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. | | |

**Trend Micro Antivirus**

|  |  |  |  |
| --- | --- | --- | --- |
| **IP** | | | |
| 99.40.40.244 | 99.40.40.223 | 99.40.40.184 | 99.40.40.182 |
| 99.40.40.181 | 99.40.40.176 | 99.40.40.172 | 99.40.40.170 |
| 99.40.40.154 | 99.40.40.152 | 99.40.40.149 | 99.40.40.141 |
| 99.40.40.133 | 99.40.40.130 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 7.1 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/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 Player < 2.0.2 Múltiples Vulnerabilidades**

|  |
| --- |
| **IP** |
| 99.40.40.223 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 7.1 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/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 ocacionar un heap-based buffer overflow, permitiendo la ejecución de código arbitrario.  - 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 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. | | |

**WinRAR < 3.71Vulnerabilidades en el Manejo de Archivos**

|  |
| --- |
| **IP** |
| 99.40.40.172 |
| 99.40.40.108 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 7.1 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:C) | La versión de WinRAR en el sistema remoto es susceptible a diversos problemas de corrupción y desbordamientos de buffer (buffer overflow). Un atacante que engañe a un usuario con un archivo malicioso podría ejecutar código con los permisos del usuario activo. |
| Solución: | | |
| Actualizar a WinRAR 3.90 o superior.  http://www.winrar.es/  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 < Múltiples vulnerabilidades**

|  |  |  |
| --- | --- | --- |
| **IP** | | |
| 99.40.40.79 | 99.40.40.244 | 99.40.40.236 |
| 99.40.40.223 | 99.40.40.191 | 99.40.40.184 |
| 99.40.40.182 | 99.40.40.181 | 99.40.40.172 |
| 99.40.40.170 | 99.40.40.154 | 99.40.40.153 |
| 99.40.40.152 | 99.40.40.149 | 99.40.40.141 |
| 99.40.40.133 | 99.40.40.130 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Medium / CVSS Base Score : 4.3  (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) | El equipo remoto contiene una versión de Adobe Flash Player que es anterior a 10.0.45.2. Estas versiones están potencialmente afectadas por múltiples vulnerabilidades:  - Un problema que podría evadir la seguridad y hacer solicitudes no autorizadas de varios dominios.  - Una denegación de servicio. |
| Solución: | | |
| Se recomienda ampliamente, instalar las actualizaciones correspondientes a Adobe Flash Player, 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 o descarga de la actualización, visite el siguiente enlace y diríjase a la sección de solución:  <http://www.adobe.com/support/security/bulletins/apsb10-06.html> | | |

**Certificados Digitales Fraudulentos podrían permitir la suplantación de identidad**

|  |
| --- |
| **IP** |
| 99.40.40.236 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Media / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) | Debido a la emisión de varios certificados SSL fraudulentos de la entidad emisora de certificados DigiNotar. Algunos de los certificados almacenados en el host remoto no son de confianza. |
| Solución: | | |
| Se recomienda quitar certificados emitidos por Diginotar del almacén de certificados.  Para más información, visite el siguiente enlace:  <http://support.microsoft.com/kb/2616676> | | |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **IP** | | | |
| 99.40.40.79 | 99.40.40.244 | 99.40.40.236 | 99.40.40.223 |
| 99.40.40.191 | 99.40.40.184 | 99.40.40.182 | 99.40.40.181 |
| 99.40.40.176 | 99.40.40.172 | 99.40.40.170 | 99.40.40.154 |
| 99.40.40.153 | 99.40.40.152 | 99.40.40.149 | 99.40.40.141 |
| 99.40.40.133 | 99.40.40.130 |

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

**Microsoft Windows Autenticación Nula en SMB**

|  |
| --- |
| **IP** |
| 99.40.40.108 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **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/ | | |

**QuickTime Múltiples desbordamiento del búfer**

|  |  |
| --- | --- |
| **IP** | |
| 99.40.40.223 | 99.40.40.184 |
| 99.40.40.176 | 99.40.40.154 |
| 99.40.40.152 | 99.40.40.149 |
| 99.40.40.141 | 99.40.40.133 |
| 99.40.40.130 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Media / CVSS Base Score : 6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P) | Un desbordamiento de buffer existe en el manejar RTSP URL de la versión de Quicktime instalada en el equipo remoto. Utilizando HTML, JavaScript o un archivo QTU como vector de ataque y una dirección RTSP URL con una larga ruta de componentes, un atacante remoto puede ser capaz de aprovechar este problema para ejecutar código arbitrario en el equipo sujeto a los privilegios del usuario. |
| Solución: | | |
| Aplicar el parche de seguridad Apple Security Update 2007-001, el cual se encuentra disponible en la aplicación: Apple Software Update, instalada en las más recientes versiones de QuickTime o iTunes.  Para más información o descarga de la actualización, visite el siguiente enlace: http://www.apple.com/support/quicktime/  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Oracle Sun Java Web Start JNLP | JRE Múltiples Vulnerabilidades**

|  |
| --- |
| **IP** |
| 99.40.40.79 |
| 99.40.40.244 |
| 99.40.40.181 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Media / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/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. | | |

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

|  |  |  |
| --- | --- | --- |
| **IP** | | |
| 99.40.40.79 | 99.40.40.244 | 99.40.40.236 |
| 99.40.40.223 | 99.40.40.191 | 99.40.40.184 |
| 99.40.40.182 | 99.40.40.181 | 99.40.40.176 |
| 99.40.40.172 | 99.40.40.170 | 99.40.40.154 |
| 99.40.40.153 | 99.40.40.152 | 99.40.40.149 |
| 99.40.40.141 | 99.40.40.133 | 99.40.40.130 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Media**  Medio / 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** | |
| 99.40.40.172 | 99.40.40.170 |
| 99.40.40.153 | 99.40.40.152 |
| 99.40.40.146 | 99.40.40.140 |
| 99.40.40.133 | 99.40.40.130 |
| 99.40.40.108 |

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

**Almacenamiento de Credenciales en Memoria**

|  |  |  |  |
| --- | --- | --- | --- |
| **IP** | | | |
| 99.40.40.79 | 99.40.40.244 | 99.40.40.236 | 99.40.40.223 |
| 99.40.40.191 | 99.40.40.184 | 99.40.40.182 | 99.40.40.181 |
| 99.40.40.176 | 99.40.40.172 | 99.40.40.170 | 99.40.40.154 |
| 99.40.40.153 | 99.40.40.152 | 99.40.40.149 | 99.40.40.141 |
| 99.40.40.133 | 99.40.40.130 | 99.40.40.108 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Baja**  Bajo / 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** | |
| 99.40.40.172 | 99.40.40.170 |
| 99.40.40.153 | 99.40.40.152 |
| 99.40.40.146 | 99.40.40.140 |
| 99.40.40.133 | 99.40.40.130 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/3389** | **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". | | |

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

|  |
| --- |
| **IP** |
| 99.40.40.140 |
| 99.40.40.135 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/3389** | **Baja**  CVSS Base Score : 2.6  (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N) | 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. | | |