**ActiveX Conjunto de actualizaciones**

|  |
| --- |
| IP |
| 99.92.176.73 |
| 99.92.176.66 |
| 99.92.176.60 |
| 99.92.176.48 |
| 99.92.176.230 |

|  |  |  |
| --- | --- | --- |
| **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> | | |

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

|  |
| --- |
| **IP** |
| 99.92.176.230 |

|  |  |  |
| --- | --- | --- |
| **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** |
| 99.92.176.60 |

|  |  |  |
| --- | --- | --- |
| **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** |
| 99.92.176.230 |

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

**Windows Service Pack fuera de tiempo**

|  |
| --- |
| **IP** |
| 99.92.176.230 |

|  |  |  |
| --- | --- | --- |
| **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 | | |

**RealPlayer < 15.0.2.71 Múltiples Vulnerabilidades (para Windows)**

|  |
| --- |
| **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) | De acuerdo al numero de la versión de RealPlayer, esta es menor a la versión 15.0.2.71. Dicha versión se ve afectada por múltiples vulnerabilidades:  - Existe un error relacionado con las banderas 'rvrender RMFF', el tamaño de los arreglos en 'RV20', 'VIDOBJ\_START\_CODE', 'RV40', 'RV10', y la decodificación en 'coded\_frame\_size' 'Atrac' podrían ocasionar ejecución de código arbitrario.  (CVE-2012-0922, CVE-2012-0923, CVE-2012-0924, CVE-2012-0925, CVE-2012-0926, CVE-2012-0927, CVE-2012-0928) |
| Solución: | | |
| Actualizar a RealPlayer 15.0.2.71 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 < 1.1.9 presenta múltiples vulnerabilidades**

|  |
| --- |
| **IP** |
| 99.92.176.230 |

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

**Windows Service Pack fuera de tiempo**

|  |
| --- |
| **IP** |
| 99.92.176.230 |

|  |  |  |
| --- | --- | --- |
| **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 | | |

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

|  |
| --- |
| **IP** |
| 99.92.176.230 |

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

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

|  |
| --- |
| **IP** |
| 99.92.176.230 |

|  |  |  |
| --- | --- | --- |
| **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) | 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 | | |

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

|  |
| --- |
| **IP** |
| 99.92.176.230 |

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

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

|  |
| --- |
| **IP** |
| 99.92.176.66 |
| 99.92.176.37 |

|  |  |  |
| --- | --- | --- |
| **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 Services. |
| 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** |
| 99.92.176.73 |
| 99.92.176.66 |
| 99.92.176.60 |
| 99.92.176.48 |
| 99.92.176.230 |

|  |  |  |
| --- | --- | --- |
| **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** |
| 99.92.176.66 |
| 99.92.176.37 |

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

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

|  |
| --- |
| **IP** |
| 99.92.176.66 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **UDP/General** | **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 cifrarlo archivos de respaldo a través de un ataque de fuerza bruta. |
| Solución: | | |
| Actualizar a BlackBerry Desktop Software 6.0.1 o posterior. | | |