**ActiveX Conjunto de actualizaciones**

|  |
| --- |
| IP |
| 99.40.24.86 |
| 99.40.24.201 |
| 99.40.24.200 |
| 99.40.24.125 |
| 99.40.24.120 |
| 99.40.24.119 |
| 99.40.24.118 |

|  |  |  |
| --- | --- | --- |
| **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 | |
| 99.40.24.86 | 99.40.24.244 |
| 99.40.24.237 | 99.40.24.201 |
| 99.40.24.179 | 99.40.24.173 |
| 99.40.24.170 | 99.40.24.164 |
| 99.40.24.125 |

|  |  |  |
| --- | --- | --- |
| **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** | | | |
| 99.40.24.86 | 99.40.24.244 | 99.40.24.237 | 99.40.24.225 |
| 99.40.24.212 | 99.40.24.201 | 99.40.24.193 | 99.40.24.179 |
| 99.40.24.174 | 99.40.24.173 | 99.40.24.171 | 99.40.24.170 |
| 99.40.24.168 | 99.40.24.122 | 99.40.24.120 | 99.40.24.118 |

|  |  |  |
| --- | --- | --- |
| **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** | | |
| 99.40.24.251 | 99.40.24.237 | 99.40.24.225 |
| 99.40.24.212 | 99.40.24.193 | 99.40.24.179 |
| 99.40.24.174 | 99.40.24.173 | 99.40.24.171 |
| 99.40.24.170 | 99.40.24.168 | 99.40.24.164 |
| 99.40.24.118 |

|  |  |  |
| --- | --- | --- |
| **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** | | |
| 99.40.24.251 | 99.40.24.237 | 99.40.24.225 |
| 99.40.24.212 | 99.40.24.193 | 99.40.24.179 |
| 99.40.24.174 | 99.40.24.173 | 99.40.24.171 |
| 99.40.24.170 | 99.40.24.168 | 99.40.24.164 |
| 99.40.24.118 |

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

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

|  |  |  |
| --- | --- | --- |
| **IP** | | |
| 99.40.24.251 | 99.40.24.244 | 99.40.24.237 |
| 99.40.24.225 | 99.40.24.212 | 99.40.24.193 |
| 99.40.24.179 | 99.40.24.174 | 99.40.24.173 |
| 99.40.24.171 | 99.40.24.170 | 99.40.24.168 |
| 99.40.24.164 | 99.40.24.122 | 99.40.24.118 |

|  |  |  |
| --- | --- | --- |
| **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** | | |
| 99.40.24.86 | 99.40.24.251 | 99.40.24.244 |
| 99.40.24.225 | 99.40.24.212 | 99.40.24.201 |
| 99.40.24.193 | 99.40.24.179 | 99.40.24.174 |
| 99.40.24.173 | 99.40.24.171 | 99.40.24.170 |
| 99.40.24.168 | 99.40.24.164 | 99.40.24.122 |
| 99.40.24.120 | 99.40.24.118 |

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

**Trend Micro Antivirus**

|  |  |  |
| --- | --- | --- |
| **IP** | | |
| 99.40.24.86 | 99.40.24.251 | 99.40.24.244 |
| 99.40.24.237 | 99.40.24.200 | 99.40.24.193 |
| 99.40.24.171 | 99.40.24.170 | 99.40.24.168 |
| 99.40.24.164 | 99.40.24.125 | 99.40.24.122 |
| 99.40.24.120 | 99.40.24.119 | 99.40.24.118 |

|  |  |  |
| --- | --- | --- |
| **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 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.  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** |
| 99.40.24.86 |

|  |  |  |
| --- | --- | --- |
| **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 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** | | | |
| 99.40.24.118 | 99.40.24.118 | 99.40.24.118 | 99.40.24.118 |
| 99.40.24.120 | 99.40.24.120 | 99.40.24.120 | 99.40.24.120 |
| 99.40.24.122 | 99.40.24.122 | 99.40.24.122 | 99.40.24.122 |
| 99.40.24.168 | 99.40.24.168 | 99.40.24.168 | 99.40.24.168 |

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

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

|  |
| --- |
| **IP** |
| 99.40.24.86 |

|  |  |  |
| --- | --- | --- |
| **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 commonNAme (CN) del certificado SSL presentadno en este puerto es diferente al del equipo. |
| Solución: | | |
| Generar un nuevo certificado digital para el servicio. | | |

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

|  |
| --- |
| **IP** |
| 99.40.24.125 |
| 99.40.24.86 |

|  |  |  |
| --- | --- | --- |
| **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) | 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** | | |
| 99.40.24.118 | 99.40.24.164 | 99.40.24.168 |
| 99.40.24.170 | 99.40.24.171 | 99.40.24.173 |
| 99.40.24.174 | 99.40.24.179 | 99.40.24.193 |
| 99.40.24.212 | 99.40.24.225 | 99.40.24.237 |
| 99.40.24.251 |

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

**Macrovision SafeDisc Desbordamiento de memoria local**

|  |
| --- |
| **IP** |
| 99.40.24.201 |

|  |  |  |
| --- | --- | --- |
| **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) | 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 superior.  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** |
| 99.40.24.119 |
| 99.40.24.125 |
| 99.40.24.200 |
| 99.40.24.201 |
| 99.40.24.86 |

|  |  |  |
| --- | --- | --- |
| **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/>  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Permisos de escritura / lectura en el servicio de NNTP**

|  |
| --- |
| **IP** |
| 99.40.24.119 |

|  |  |  |
| --- | --- | --- |
| **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 servidor remoto parece estar abierto a los usuarios remotos. Algunos usuarios prefieren el acceso público de servidores NNTP para leer y publicar artículos de forma anónima.  Conexiones no deseadas pueden afectar el ancho de banda de su red o ponerle en problemas legales si una persona malintencionada usa su servidor para publicar mensajes. |
| Solución: | | |
| Exigir la autenticación de usuario o filtrar las conexiones desde el exterior en el dispositivo de seguridad perimetral. | | |

**SSL Protocolo de cifrado inseguro**

|  |
| --- |
| **IP** |
| 99.40.24.86 |

|  |  |  |
| --- | --- | --- |
| **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) | 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 Web Start JNLP problemas de desbordamiento de búfer | JRE DoS en librería dinámica jpiexp32.dll**

|  |
| --- |
| **IP** |
| 99.40.24.86 |
| 99.40.24.201 |

|  |  |  |
| --- | --- | --- |
| **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) | 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** | | |
| 99.40.24.118 | 99.40.24.120 | 99.40.24.122 |
| 99.40.24.164 | 99.40.24.168 | 99.40.24.170 |
| 99.40.24.171 | 99.40.24.173 | 99.40.24.174 |
| 99.40.24.179 | 99.40.24.193 | 99.40.24.212 |
| 99.40.24.225 | 99.40.24.237 | 99.40.24.244 |
| 99.40.24.251 |

|  |  |  |
| --- | --- | --- |
| **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** | | |
| 99.40.24.118 | 99.40.24.119 | 99.40.24.120 |
| 99.40.24.121 | 99.40.24.125 | 99.40.24.168 |
| 99.40.24.179 | 99.40.24.200 | 99.40.24.201 |
| 99.40.24.245 | 99.40.24.251 | 99.40.24.50 |
| 99.40.24.86 |

|  |  |  |
| --- | --- | --- |
| **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** | | | | |
| 99.40.24.118 | 99.40.24.119 | 99.40.24.120 | 99.40.24.122 | 99.40.24.125 |
| 99.40.24.154 | 99.40.24.164 | 99.40.24.168 | 99.40.24.170 | 99.40.24.171 |
| 99.40.24.173 | 99.40.24.174 | 99.40.24.179 | 99.40.24.193 | 99.40.24.200 |
| 99.40.24.201 | 99.40.24.212 | 99.40.24.225 | 99.40.24.237 | 99.40.24.244 |
| 99.40.24.251 | 99.40.24.86 |

|  |  |  |
| --- | --- | --- |
| **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** | | |
| 99.40.24.118 | 99.40.24.119 | 99.40.24.120 |
| 99.40.24.121 | 99.40.24.125 | 99.40.24.168 |
| 99.40.24.179 | 99.40.24.200 | 99.40.24.201 |
| 99.40.24.245 | 99.40.24.251 | 99.40.24.50 |
| 99.40.24.86 |

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

|  |
| --- |
| **IP** |
| 99.40.24.86 |

|  |  |  |
| --- | --- | --- |
| **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) | moto 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** |
| 99.40.24.86 |

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

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

|  |
| --- |
| **IP** |
| 99.40.24.119 |
| 99.40.24.200 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/21** | **Baja**  CVSS Base Score : 2.6  (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N) | El sistema remoto ejecuta el servicio de FTP, este servicio para transferencia de archivos transmite la información del usuario en texto claro, por lo que es posible interceptar las credenciales de accesos al servicio, así como los datos a través de un ataque de hombre en medio (MiTM) por medio de un sniffer en el segmento de red donde se produce la comunicación. |
| Solución: | | |
| Utilizar SFTP en lugar de este servicio o filtrar el trafico entrante al puerto o encapsular el trafico en un canal de SSL. | | |

**Nessus UDP scanner**

|  |
| --- |
| **IP** |
| 99.40.24.238 |
| 99.40.24.227 |
| 99.40.24.172 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/21** | **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. | | |