**ActiveX Conjunto de actualizaciones**

|  |
| --- |
| IP |
| 99.51.32.147 |
| 99.51.32.126 |

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

**Apache < 1.3.28 Múltiples Vulnerabilidades**

|  |
| --- |
| **IP** |
| 99.51.32.157 |

|  |  |  |
| --- | --- | --- |
| **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) | El equipo remoto parece estar ejecutando una versión de Apache, que es mayor de 1.3.28  Existen diferentes errores en esta versión, incluyendo una denegación de servicio en el manejo de caracteres de control en la utilidad "rotatelogs" y la perdida de archivos en el manejo de módulos de terceros. |
| Solución: | | |
| Actualizar a la versión 1.3.28 o el más reciente. Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Detección de servidor web obsoleto**

|  |
| --- |
| **IP** |
| 99.51.32.157 |

|  |  |  |
| --- | --- | --- |
| **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) | De acuerdo con la versión detectada del servidor web remoto, esta es obsoleta y ya no cuenta más con mantenimiento por parte del vendedor o fabricante. |
| Solución: | | |
| Cambiar a una versión mas nueva o cambiar a otro servidor, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

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

|  |
| --- |
| **IP** |
| 99.51.32.157 |

|  |  |  |
| --- | --- | --- |
| **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) | Es posible obtener el nombre de la comunidad por default: "public" esta configurada en el agente del protocolo SNMP. Un atacante remoto puede utilizar esta mala configuración para obtener información sensible del sistema afectado. |
| Solución: | | |
| Cambiar el nombre de la comunidad a una personalizada por el administrador del servicio, si es posible, configurar la versión 3 de SNMP, que incluye un mecanismo de cifrado para las respuestas del servicio.  Evaluar si el servicio no es necesario y en su defecto deshabilitarlo. | | |

**Microsoft Windows Update necesita ser reiniciado**

|  |
| --- |
| **IP** |
| 99.51.32.126 |

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

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

|  |
| --- |
| **IP** |
| 99.51.32.147 |
| 99.51.32.126 |

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

### SNMP los nombres de comunidad del servidor remoto pueden ser adivinados

|  |
| --- |
| **IP** |
| 99.51.32.157 |

|  |  |  |
| --- | --- | --- |
| **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 nombre de la comunidad SNMP en el sistema remoto, está establecido con el nombre por defecto (public), a través de este servicio un atacante puede obtener información importante del sistema. |
| Solución: | | |
| Validar el uso del servicio. Si el servicio no es requerido, consultar la documentación del fabricante sobre la desactivación del servicio. Si es requerido entonces establecer un filtrado para la conexión al puerto/servicio y cambiar el nombre de la comunidad SNMP por defecto. | | |

**Trend Micro Antivirus**

|  |
| --- |
| **IP** |
| 99.51.32.147 |
| 99.51.32.126 |

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

**Apache < 2.3.41 múltiples vulnerabilidades**

|  |
| --- |
| **IP** |
| 99.51.32.157 |
| 99.51.32.155 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/80**  **TCP/8080** | **Media**  Media / CVSS Base Score : 4.3 (VSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) | De acuerdo al banner la versión de Apache 2.2 es menor a la versión 2.2.23. Por lo tanto se ve afectada por múltiples problemas de seguridad:  - La utilidad 'apachectl' puede recibir un nombre de directorio LD\_LIBRARY\_PATH de longitud cero en 'envvars' mediante un archivo. Un atacante local podría explotar esta vulnerabilidad y cargar algún Dynamic Shared Object (DSO) malicioso permitiendo la ejecución remota de código. (CVE-2012-0883)  - Problemas en la validación de 'mod\_negotiation', 'Multiviews' podría permitir ataques del tipo cross-site scripting. (CVE-2012-2687) |
| Solución: | | |
| Actualizar a la versión de Apache 2.2.24 o superior. O validar que no se este utilizando el modulo que se ve afectado.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado | | |

**Apache IBM HTTP server Vulnerable a cross-site scripting (XSS)**

|  |
| --- |
| **IP** |
| 99.51.32.157 |

|  |  |  |
| --- | --- | --- |
| **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) | El servidor remoto falla al sanitizar el contenido de los encabezados esperados de las peticiones del usuario antes de utilizarlas para generar contenido dinámico. Un atacante puede aprovechar este problema para efectuar un ataque de cross-site scripting contra el servicio afectado, mediante archivos ShockWave (SWF) maliciosos. |
| Solución: | | |
| Actualizar el servidor a la versión mas nueva del aplicativo según corresponda:  Apache 1.3.41 / 2.0.63 / 2.2.14 o posterior. http://httpd.apache.org/  IBM HTTP Server 6.0.2.13 / 6.1.0.1 o posterior.  IBM WebSphere Application Server 5.1.1.17 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. | | |

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

|  |
| --- |
| **IP** |
| 99.51.32.126 |

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

**Servidor WEB Genérico Funciones de debug habilitadas**

|  |
| --- |
| **IP** |
| 99.51.32.157 |
| 99.51.32.155 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Media**  Media / CVSS Base Score : 4.3 (VSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) | El servidor remoto tiene habilitados los métodos HTTP TRACE y/o TRACK habilitados, estos métodos son utilizados para realizar depuración de las conexión al servidor. Estos métodos pueden ser aprovechados por un atacante para realizar una ejecución cruzada de código. |
| Solución: | | |
| Consultar al fabricante y deshabilitar los métodos no requeridos en el servidor WEB. | | |

**SSL Protocolo de cifrado inseguro**

|  |
| --- |
| **IP** |
| 99.51.32.126 |

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

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

|  |  |  |
| --- | --- | --- |
| **IP** | | |
| 99.51.32.81 | 99.51.32.153 | 99.51.32.130 |
| 99.51.32.77 | 99.51.32.152 | 99.51.32.129 |
| 99.51.32.191 | 99.51.32.143 | 99.51.32.128 |
| 99.51.32.190 | 99.51.32.142 | 99.51.32.127 |
| 99.51.32.185 | 99.51.32.141 | 99.51.32.121 |
| 99.51.32.181 | 99.51.32.140 | 99.51.32.120 |
| 99.51.32.180 | 99.51.32.136 |
| 99.51.32.159 | 99.51.32.134 |
| 99.51.32.155 | 99.51.32.133 |
| 99.51.32.154 | 99.51.32.132 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/3389** | **Media**  Media / CVSS Base Score : 5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P) | El servicio Terminal Services en el host remoto es propenso a un ataque de hombre en medio y robo de sesión con lo cual un atacante podría obtener acceso al sistema con las credenciales del usuario conectado vía Terminal Service. |
| Solución: | | |
| Forzar el uso de SSL en las conexiones. Si no es posible crear un túnel de ssh para el uso del servicio. | | |

**Uso de llaves débiles para cifrado SSL**

|  |
| --- |
| **IP** |
| 99.51.32.1 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/443** | **Media**  Media / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N) | El sistema remoto soporta el uso de llaves SSL débiles (56bits >= 112bits) que ofrecen un cifrado débil para la comunicación de los datos. |
| Solución: | | |
| Deshabilitar el soporte para SSL 2.0 y utilizar SSL3.0 o TLS 1.0 en su lugar. En el archivo de configuración httpd.conf o ssl.conf según corresponda, establecer.  SSLProtocol -ALL +SSLv3 +TLSv1  SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:-LOW:-SSLv2:-EXP | | |

**Almacenamiento de credenciales en memoria**

|  |
| --- |
| **IP** |
| 99.51.32.147 |
| 99.51.32.126 |

|  |  |  |
| --- | --- | --- |
| **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** | | |
| 99.51.32.81 | 99.51.32.154 | 99.51.32.132 |
| 99.51.32.77 | 99.51.32.153 | 99.51.32.130 |
| 99.51.32.191 | 99.51.32.152 | 99.51.32.129 |
| 99.51.32.190 | 99.51.32.143 | 99.51.32.128 |
| 99.51.32.185 | 99.51.32.142 | 99.51.32.127 |
| 99.51.32.181 | 99.51.32.141 | 99.51.32.121 |
| 99.51.32.180 | 99.51.32.140 | 99.51.32.120 |
| 99.51.32.159 | 99.51.32.136 |
| 99.51.32.155 | 99.51.32.134 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/3389** | **Baja**  Baja / CVSS Base Score : 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N) | El nivel de cifrado utilizado en el servicio de escritorio remoto no es FIPS-140 compliant. |
| Solución: | | |
| Establecer el nivel de cifrado del protocolo RDP a 4 "FIPS Compliant". | | |

**Servicio Telnet**

|  |
| --- |
| **IP** |
| 99.51.32.87 |
| 99.51.32.86 |
| 99.51.32.85 |
| 99.51.32.84 |
| 99.51.32.83 |
| 99.51.32.82 |
| 99.51.32.1 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Baja** | El sistema remoto está ejecutando el servicio telnet. Este servicio es usado para la administración remota de equipos. La arquitectura de este servicio, lo hace inseguro ya que la comunicación en el cliente y el servidor se lleva a cabo sin ningún cifrado, esto lo hace propenso a ataques de robo de sesión, el cual permite tomar control total del sistema. |
| Solución: | | |
| Validar el uso del servicio, en caso de no ser necesario, consultar al fabricante sobre la des habilitación del servicio, si es requerido entonces establecer un filtrado para la conexión al puerto/servicio. | | |

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

|  |
| --- |
| **IP** |
| 99.51.32.1 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/443** | **Baja** | El sistema remoto utiliza un certificado digital SSL que a sido firmado utilizando una algoritmo de hash (digestión) débil como MD2, MD4, o MD5. Estos algoritmos son vulnerables a un ataque de colisión, lo que puede permitir a un atacante generar un certificado con el mismo hash (digestión) que el original y de esta manera suplantar identidades y captar trafico cifrado. |
| Solución: | | |
| Solicitar un nuevo certificado a la entidad certificadora correspondiente. | | |