**Acceso a recursos compartidos**

|  |
| --- |
| IP |
| 99.92.44.37 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 7.5 (CVSS2#AV:N AC:L/Au:N/C:P I:P/A:P) | Es posible acceder a los recursos compartidos vía SMB con las credenciales provistas. Dependiendo de los permisos, esto puede permitirá un atacante a leer/escribir información confidencial. |
| Solución: | | |
| Establecer permisos específicos de acceso, lectura y escritura para cada usuario que requiera utilizar los recursos. | | |

**ActiveX Conjunto de actualizaciones**

|  |
| --- |
| IP |
| 99.92.44.97 |
| 99.92.44.16 |
| 99.92.44.104 |

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

**Microsoft Office Service Pack desactualizado**

|  |
| --- |
| **IP** |
| 99.92.44.104 |

|  |  |  |
| --- | --- | --- |
| **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 Microsoft Office no tiene service pack o el que tiene ya no es soportado actualmente. |
| Solución: | | |
| Instalar la última versión de service pack.  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** |
| 99.92.44.97 |
| 99.92.44.16 |

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

**Trend Micro Antivirus**

|  |
| --- |
| **IP** |
| 99.92.44.97 |
| 99.92.44.16 |

|  |  |  |
| --- | --- | --- |
| **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 < 3.71Múltiples Vulnerabilidades**

|  |
| --- |
| **IP** |
| 99.92.44.104 |

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

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

|  |
| --- |
| **IP** |
| 99.92.44.4 |
| 99.92.44.26 |
| 99.92.44.19 |
| 99.92.44.17 |
| 99.92.44.104 |

|  |  |  |
| --- | --- | --- |
| **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** |
| 99.92.44.97 |
| 99.92.44.16 |
| 99.92.44.104 |

|  |  |  |
| --- | --- | --- |
| **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** |
| 99.92.44.4 |
| 99.92.44.26 |
| 99.92.44.19 |
| 99.92.44.17 |
| 99.92.44.104 |

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