**Acceso a recursos compartidos**

|  |
| --- |
| IP |
| 99.40.16.129 |

|  |  |  |
| --- | --- | --- |
| **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) | 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 |
| 99.40.16.139 |

|  |  |  |
| --- | --- | --- |
| **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 / 9.5.1 Múltiples Vulnerabilidades (APSB12-08)**

|  |
| --- |
| IP |
| 99.40.20.230 |
| 99.40.20.60 |

|  |  |  |
| --- | --- | --- |
| **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 de Adobe Reader instalada en el equipo remoto es menor a la versión 10.1.3 / 9.5.1, estas versiones se ven afectadas por múltiples vulnerabilidades:  - Un desbordamiento de enteros existe en las fuentes de letras True Type Font (TFF). (CVE-2012-0774)  - Una vulnerabilidad de corrupción de memoria existe en el manejador de JavaScript. (CVE-2012-0775)  - Un problema de seguridad existe en Adobe Reader installer el cual podría ocasionar la evasión a ciertas restricciones de seguridad.  (CVE-2012-0776) |
| Solución: | | |
| Actualizar a Adobe Reader 9.5.1 / 10.1.3 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** |
| 99.40.16.139 |

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

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

|  |
| --- |
| **IP** |
| 99.40.16.133 |

|  |  |  |
| --- | --- | --- |
| **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** |
| 99.40.16.139 |

|  |  |  |
| --- | --- | --- |
| **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** |
| 99.40.16.133 |

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

**Altas**

MS 2695962: Actualización para ActiveX en sus Kill Bits (2695962)

MS KB2719662: Vulnerabilidades en Gadgets podría permitir la ejecución de código remoto

MS08-069: Ejecución remota de código sobre Microsoft XML Core Services (955218)

MS10-012: Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código

MS11-007: Vulnerabilidad en el controlador del OpenType Compact Font Format (CFF) podría permitir la ejecución remota de código

MS11-015: Vulnerabilidades en Windows Media podrían permitir la ejecución remota de código

MS11-019: Vulnerabilidades en SMB Client permiten la ejecución de código remoto.

MS11-020: SMB presenta fallas en su implementación que permite la ejecución de código remoto

MS11-020: Vulnerabilidad en SMB server podría resultar en ejecución remota de código (2508429)

MS11-024: Vulnerabilidad en el editor Windows Fax Cover Page permite la ejecución de código remoto.

MS11-027: Actualización de seguridad acumulativa para ActiveX

MS11-030: Vulnerabilidad en la resolución DNS podría permitir la ejecución remota de código

MS11-031: Vulnerabilidad en los motores de scripting de JScript y VBScript podría permitir la ejecución remota de código.

MS11-032: Vulnerabilidad en el controlador OpenType Compact Font Format (CFF) podría permitir la ejecución remota de código.

MS11-038: Vulnerabilidades en OLE Automation podrían permitir ejecución de código remoto (2476490)

MS11-043: Una vulnerabilidad en el cliente SMB podrían permitir la ejecución remota de código (2536276)

MS11-046: Vulnerabilidad en Ancillary Function Driver podría permitir ejecución de código remota (2503665)

MS11-048: Vulnerabilidad en SMB Server podría ocasionar una denegación de servicio (2536275)

MS11-048: Vulnerabilidad en SMB Server podría permitir una denegación de servicio (2536275)

MS11-071 Vulnerabilidad en componentes de windows podría permitir ejecución de código de manera remota.

MS11-075: Vulnerabilidad en Microsoft Active Accessibility podría permitir la ejecución remota de código (2623699)

MS11-076: Vulnerabilidad en Windows Media Center podría permitir la ejecución remota (2604926)

MS11-085: Vulnerabilidad en Windows Mail and Windows Meeting Space podría permitir la ejecución remota de código (2620704)

MS11-090: Actualización de seguridad para ActiveX

MS11-092: Una vulnerabilidad en Windows Media podría permitir la ejecución remota de código

MS11-097: Una vulnerabilidad en el subsistema de Windows en tiempo de ejecuciÃ³n cliente / servidor podría permitir la elevaciÃ³n de privilegios

MS12-074: Vulnerabilidad en .NET Framework podría permitir la ejecución de código remoto (2745030)

MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)

MS12-081: Vulnerabilidad en Windows en el componente de manejo de archivos podría permitir la ejecución de código remoto (2758857)

MS12-082: Vulnerabiloidad en DirectPlay podría permitir la ejecución de código remoto (2770660)

MS13-001: Vulnerabilidad en Windows Print Spooler Components podría permitir la ejecución remota de código (2769369)

MS13-002: Vulnerabilidad en Microsoft XML podría permitir la ejecución de código remoto (2756145)

MS13-004: Vulnerabilidad en .NET Framework podría permitir la elevación de privilegios (2769324)

MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277)

MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113)

MS13-021: Actualizaciones de seguridad para Internet Explorer (2809289)

MS13-022: Vulnerabilidad en Microsoft Silverlight podría permitir ejecución de código remoto (2814124)

MS13-027: Vulnerabilidad en Kernel-Mode Drivers podría permitir elevación de privilegios de seguridad (2807986)

**Medias**

MS 2647518: Actualización para ActiveX Kill Bits (2647518)

MS KB2728973: Certificados digitales no autorizados podrían permitir la suplantación de identidad

MS11-009: Vulnerabilidad los motores de scripting de JScript y VBScript podrían permitir la divulgación de información

MS11-026: Vulnerabilidad en MHTML podría permitir la divulgación de información

MS11-037: Múltiples Vulnerabilidades en MHTML podrían permitir revelación de información (2544893)

MS11-066: Una vulnerabilidad en el control Microsoft Chart podría permitir la divulgación de información

MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)

MS13-006: Vulnerabilidad en Microsoft Windows podría permitir la evasión de restricciones de seguridad (2785220)

MS13-007: Vulnerabilidad en Open Data Protocol podría permitir una denegación de servicio (2769327)