|  |  |  |  |
| --- | --- | --- | --- |
| **Responsable del proyecto por parte de CLIENTE** | **Elaboró - DSA** | **Revisó - DSA** | **Aprobó – DSA**  **TAM - DSA** |
| Nombre del responsable | Armin García | Frank Ortiz | Jesús Santiago Ávila |
|  |  |  |  |
| Fecha de firma: | | | |
| Nota: La fecha de revisión del presente reporte por parte del CLIENTE**,** vence a los 5 días después de la fecha de entrega del mismo. | | | |

[1. Objetivo del documento 3](#_Toc346726539)

[2. Introducción 3](#_Toc346726540)

[3. Alcance 3](#_Toc346726541)

[4. Definiciones 4](#_Toc346726542)

[5. Alcance del análisis 5](#_Toc346726543)

[6. Visión General 6](#_Toc346726544)

[Sección A. Descripción de las actividades realizadas: 7](#_Toc346726545)

[Sección B. Descripción del ambiente 8](#_Toc346726546)

[Sección C. Lista de equipos escaneados 9](#_Toc346726547)

[Sección D. Hallazgos 12](#_Toc346726548)

[Vulnerabilidades de prioridad Alta para CLIENTE99.40.16.0 13](#_Toc346726549)

[Vulnerabilidades de prioridad Media para CLIENTE99.40.16.0 35](#_Toc346726550)

[Vulnerabilidades de prioridad Baja para CLIENTE99.40.16.0 45](#_Toc346726551)

[Vulnerabilidades de prioridad Alta para CLIENTE99.40.20.0 47](#_Toc346726552)

[Vulnerabilidades de prioridad Media para CLIENTE99.40.20.0 73](#_Toc346726553)

[Vulnerabilidades de prioridad Baja para CLIENTE99.40.20.0 84](#_Toc346726554)

[Vulnerabilidades de prioridad Alta para CLIENTE99.40.24.0 87](#_Toc346726555)

[Vulnerabilidades de prioridad Media para CLIENTE99.40.24.0 132](#_Toc346726556)

[Vulnerabilidades de prioridad Baja para CLIENTE99.40.24.0 153](#_Toc346726557)

[Vulnerabilidades de prioridad Alta para CLIENTE99.40.40.0 158](#_Toc346726558)

[Vulnerabilidades de prioridad Media para CLIENTE99.40.40.0 192](#_Toc346726559)

[Vulnerabilidades de prioridad Baja para CLIENTE99.40.40.0 208](#_Toc346726560)

[Sección E. Recomendaciones 210](#_Toc346726561)

[ Tecnología 210](#_Toc346726562)

[ Procesos 210](#_Toc346726563)

|  |  |
| --- | --- |
| Objetivo del documento | El objetivo de este documento es proporcionar al CLIENTE los resultados de los escaneos de vulnerabilidades llevado a cabo por el Tiger Team de DSA de Scitum, resumen de actividades realizadas, hallazgos y recomendaciones para mitigar las vulnerabilidades encontradas en los equipos y servicios. |

|  |  |
| --- | --- |
| Introducción | El CLIENTE, tiene como una de sus funciones definir, difundir y supervisar el cumplimiento de las normas, políticas, estándares y procedimientos de calidad y seguridad de la información, con la finalidad de promover y mantener la integridad, precisión, confiabilidad, protección y congruencia de la información del CLIENTE.  Este documento contiene los resultados del escaneo de vulnerabilidades a diversos dispositivos del CLIENTE, basado en la premisa de mantener en niveles aceptables la percepción de riesgo de sufrir una amenaza o ataque por el aprovechamiento de vulnerabilidades. La selección de equipos fue realizada por parte del CLIENTE y se estableció un calendario para la realización de las pruebas.    Cabe mencionar que existieron diversas restricciones en la ejecución de las pruebas, debido a la criticidad de algunos equipos y los horarios planeados para el ejercicio. |

|  |  |
| --- | --- |
| Alcance | Este documento debe ser conocido por:   * + La dirección y las gerencias de Seguridad Informática del CLIENTE. * Todos los miembros que participan directamente en la planeación, implantación y monitoreo de la infraestructura tecnológica. |

|  |  |
| --- | --- |
| Definiciones | Para facilitar la lectura y comprensión de este procedimiento, se consideran las siguientes definiciones:   1. EV (Escaneo de Vulnerabilidades): Es un proyecto orientado para la obtención de información sobre las debilidades en la infraestructura del CLIENTE. 2. Nessus: Es una herramienta de código libre que se utiliza para la valoración de seguridad que verifica la vulnerabilidad a los ataques de todas las entidades accesibles de la red. También examina todos los servicios TCP/IP de la red e incluye revisiones de vulnerabilidad específica para sistemas operativos, servidores Web y Firewalls. 3. Riesgo: Probabilidad que una amenaza particular explote una vulnerabilidad particular de un sistema. 4. Ataque: Acción de tratar de traspasar controles de seguridad en un sistema. Un ataque puede ser activo, resultando en la modificación de datos, o pasivo, resultando en la divulgación de información. El hecho de que un ataque sea realizado no significa que será exitoso, el grado de éxito depende de la vulnerabilidad del sistema o actividad y de la eficiencia de las medidas existentes. 5. Vulnerabilidad: Debilidad en los procedimientos de seguridad de un sistema, en el diseño del sistema, en la implementación, en los controles internos, y que puede ser explotada para violar la política de seguridad del sistema. 6. Falso positivo: Es la probabilidad de que estando presente cierta actividad identificada en un sistema de detección de intrusos o analizador de redes en un ambiente de red y analizada como tráfico normal, el sistema de detección asuma que la actividad es sospechosa y está presente. |

# Alcance del análisis

El presente reporte incluye los resultados del análisis de vulnerabilidades llevado a cabo en el mes de enero de 2013.

El presente reporte incluye un análisis de XXX equipos de los segmentos de red para XXXX, los cuales se muestra a continuación:

|  |  |
| --- | --- |
| **Descripción** | **IP** |
| **Direccionamiento** | **Ejemplo**  **99.40.24.0/24** |
| **Ejemplo**  **99.40.20.0/24** |
| **Ejemplo**  **99.40.16.0/24** |
| **Ejemplo**  **99.40.12.0/24** |
| **Ejemplo**  **99.40.36.0/24** |
| **Ejemplo**  **99.40.40.0/24** |

Estos hallazgos se listan en la **Sección D** de este documento.

|  |  |
| --- | --- |
| Visión General |  |

La auditoría se realizó desde las instalaciones del inmueble del CLIENTE. El escaneo fue realizado en un ambiente con privilegios y direccionamiento interno, con el fin de analizar los componentes y procesos, para mostrar las debilidades de configuración y vulnerabilidades que un usuario malicioso podría aprovechar.

El estudio se considera:

* Cuantificable
* Consistente
* Repetible
* Detallado

Durante el Escaneo de Vulnerabilidades los hallazgos fueron los siguientes:

Las vulnerabilidades de criticidad Alta son causadas por las siguientes razones:

* Falta de parches de aplicación
* Falta de parches de sistema operativo
* Mala Configuración

Las vulnerabilidades de criticidad Media son causadas por las siguientes razones:

* Mala Configuración
* Falta de parches de aplicación
* Falta de Parches de Sistema Operativo
* Protocolo no seguro
* Configuración por defecto

Las vulnerabilidades de criticidad Baja son causadas por las siguientes razones:

* Mala Configuración
* Configuración por defecto

## Sección A. Descripción de las actividades realizadas:

La ejecución de escaneo de vulnerabilidades consistió en las siguientes actividades realizadas:

Las pruebas de descubrimiento de vulnerabilidades que se llevaron a cabo durante el AV a la infraestructura, fueron realizadas acorde a lo especificado por la herramienta de escaneo utilizada, en un horario de 09:00 a 18:00hrs. El 11 y 14 de enero de 2013.

* No se realizaron pruebas con denegación de servicios activadas, así como técnicas de hackeo activadas
* No se realizó implementación alguna, derivada de recomendaciones al servicio afectado
* Búsqueda y análisis de vulnerabilidades de los sistemas. Se detallan de manera enunciativa más no limitativa.

| **Aspecto evaluado con las herramientas utilizadas.** |
| --- |
|
| **Sistema Operativo** |
| **Aplicación de parches** |
| **Debilidad de contraseñas** |
| **Permisos en archivos** |
| **Barrido de puertos** |
| **Puertas traseras** |
| **Shares** |
| **SNMP** |
| **RPC** |
| **Recopilación de información (fingerprinting)** |
| **Vulnerabilidades** |
| **Fuerza bruta** |
| **CGIs** |
| **Demonios** |
| **DCOM** |
| **DNS** |
| **Correo electrónico** |
| **FTP** |
| **Recopilación de información** |
| **Aspectos críticos de S.O.** |
| **Grupos de S.O.** |
| **Red S.O** |
| **Servicios** |
| **Usuarios** |

## Sección B. Descripción del ambiente

Se escanearon XXX equipos del inmueble XXXXX dicha prueba fue realizada con privilegios y desde la red interna.

El orden en que se mostrarán los resultados será de acuerdo a la criticidad de la vulnerabilidad, de acuerdo al siguiente orden:

* **ALTA:** Equipos que de acuerdo al resultado del escaneo de vulnerabilidades, requieren de un análisis o acción inmediata. Estas vulnerabilidades deben ser corregidas de forma inmediata o en un corto plazo, ya que su presencia pone en riesgo la confidencialidad, integridad y/o disponibilidad de la información contenida en los dispositivos.
* **MEDIA:** Estas vulnerabilidades son consecuencia de una configuración predeterminada o falta de aseguramiento en los dispositivos. Su presencia no pone en riesgo inminente la integridad o confidencialidad de la información, sin embargo es necesario mitigarlas inmediatamente después de corregir las vulnerabilidades críticas.
* **BAJA:** Equipos que tienen habilitados algunos puertos de servicios comunes de acuerdo al sistema operativo y que son necesarios, pero susceptibles de sufrir alguna vulnerabilidad.
* **INFORMATIVA:** Notificaciones de sistema que no representan una vulnerabilidad, son de carácter informativo de algún puerto o servicio descubierto durante la aplicación de la prueba.

## Sección C. Lista de equipos escaneados

La siguiente tabla lista todos los equipos que fueron escaneados durante este análisis de vulnerabilidades, a continuación se proporcionan una breve descripción de los campos que la conforman:

* **IP:** Dirección IP de equipo analizado.
* **Nombre:** Nombre del host auditado.

|  |  |  |
| --- | --- | --- |
| **IP** | | **NOMBRE** |
| **99.40.16.0** | | |
| 99.40.16.61 |  | |
| 99.40.16.102 |  | |

## Sección D. Hallazgos

#### Servicios habilitados en los equipos

A continuación se muestran las vulnerabilidades encontradas después de los AV´s realizados por el equipo Tiger Team, los hallazgos encontrados fueron organizados en las siguientes categorías de riesgo, ALTA, MEDIA y BAJA.

La descripción de los campos de la tabla es la siguiente:

* + ***Nombre***: Muestra el nombre del dispositivo evaluado
  + ***Protocolo***: Identifica al protocolo por el cual está habilitado el servicio
  + ***Puerto***: Identifica la puerta de enlace por donde el servicio está habilitado.
  + ***Servicios***: Lista los servicios de red habilitados en el dispositivo evaluado
  + ***Sistema Operativo***: Versión de Sistema operativo que se identifico durante el escaneo.
  + ***Impacto*:** Describe el nivel de impacto identificado de acuerdo a la vulnerabilidad encontrada.
  + ***Descripción:*** Detalla la forma en la que se puede aprovechar la vulnerabilidad.

**Vulnerabilidades:**

**Segmento 99.40.16.0**

### Vulnerabilidades de prioridad Alta para CLIENTE99.40.16.0

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.137 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2695962: Actualización para ActiveX en sus Kill Bits (2695962)  MS KB2269637: Carga insegura de librerías podría permitir ejecución remota de código  MS KB2719662: Vulnerabilidades en Gadgets podría permitir la ejecución de código remoto  MS10-033: Vulnerabilidades en la descompresión de archivos multimedia, podrían permitir la ejecución remota de código(979902)  MS10-044: Vulnerabilidades en Microsoft Office Access ActiveX Controls podrían permitir la ejecución remota de código (982335)  MS10-055: Vulnerabilidad en códec multimedia Cinepak podría permitir la ejecución remota de código (982665)  MS10-059: Vulnerabilidades en la función de seguimiento para los servicios podrían permitir elevación de privilegios  MS10-060: Vulnerabilidades en Microsoft NET Common Language Runtime y en Microsoft Silverlight de podrían permitir la ejecución remota de código  MS10-082: Vulnerabilidad en Windows Media Player, podría permitir la ejecución remota de código (2378111)  MS10-083: Una vulnerabilidad en la validación COM en el shell de Windows y WordPad, podría permitir la ejecución remota de código (2405882)  MS11-091: Vulnerabilidad en Microsoft Publisher podría permitir la ejecución remota de código  MS12-039: Vulnerabilidad en Lync podría permitir la ejecución de código remoto (2707956)  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  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)  MS13-005: Vulnerabilidad en Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2778930) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.138 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2695962: Actualización para ActiveX en sus Kill Bits (2695962)  MS KB2269637: Carga insegura de librerías podría permitir ejecución remota de código  MS KB2719662: Vulnerabilidades en Gadgets podría permitir la ejecución de código remoto  MS09-060: Vulnerabilidades en Controles ActiveX de Microsoft Active Template Library (ATL) para Microsoft Office podrían permitir la ejecución remota de código (973965)  MS10-033: Vulnerabilidades en la descompresión de archivos multimedia, podrían permitir la ejecución remota de código(979902)  MS10-044: Vulnerabilidades en Microsoft Office Access ActiveX Controls podrían permitir la ejecución remota de código (982335)  MS10-055: Vulnerabilidad en códec multimedia Cinepak podría permitir la ejecución remota de código (982665)  MS10-059: Vulnerabilidades en la función de seguimiento para los servicios podrían permitir elevación de privilegios  MS10-082: Vulnerabilidad en Windows Media Player, podría permitir la ejecución remota de código (2378111)  MS10-083: Una vulnerabilidad en la validación COM en el shell de Windows y WordPad, podría permitir la ejecución remota de código (2405882)  MS11-039: Vulnerabilidad en .NET y Microsoft Silverlight podría permitir ejecución remota de código (2514842)  MS11-078: Vulnerabilidad en .NET Framework y Microsoft Silverlight podría permitir ejecución remota de código (2604930)  MS11-091: Vulnerabilidad en Microsoft Publisher podría permitir la ejecución remota de código  MS12-034: Actualizaciones de Seguridad para Microsoft Office, Windows, .NET Framework, y Silverlight (2681578)  MS12-039: Vulnerabilidad en Lync podría permitir la ejecución de código remoto (2707956)  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  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)  MS13-005: Vulnerabilidad en Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2778930) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.145 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2695962: Actualización para ActiveX en sus Kill Bits (2695962)  MS KB2269637: Carga insegura de librerías podría permitir ejecución remota de código  MS KB2719662: Vulnerabilidades en Gadgets podría permitir la ejecución de código remoto  MS10-033: Vulnerabilidades en la descompresión de archivos multimedia, podrían permitir la ejecución remota de código(979902)  MS10-044: Vulnerabilidades en Microsoft Office Access ActiveX Controls podrían permitir la ejecución remota de código (982335)  MS10-055: Vulnerabilidad en códec multimedia Cinepak podría permitir la ejecución remota de código (982665)  MS10-059: Vulnerabilidades en la función de seguimiento para los servicios podrían permitir elevación de privilegios  MS10-060:. Vulnerabilidades en Microsoft NET Common Language Runtime y en Microsoft Silverlight de podrían permitir la ejecución remota de código  MS10-082: Vulnerabilidad en Windows Media Player, podría permitir la ejecución remota de código (2378111)  MS10-083: Una vulnerabilidad en la validación COM en el shell de Windows y WordPad, podría permitir la ejecución remota de código (2405882)  MS11-091: Vulnerabilidad en Microsoft Publisher podría permitir la ejecución remota de código  MS12-039: Vulnerabilidad en Lync podría permitir la ejecución de código remoto (2707956)  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  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)  MS13-005: Vulnerabilidad en Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2778930) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.156 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2695962: Actualización para ActiveX en sus Kill Bits (2695962)  MS KB2269637: Carga insegura de librerías podría permitir ejecución remota de código  MS KB2719662: Vulnerabilidades en Gadgets podría permitir la ejecución de código remoto  MS09-059: Vulnerabilidad en LSSAS (Local Security Authority Subsystem Servic) podría permitir una denegación de servicio  MS10-033: Vulnerabilidades en la descompresión de archivos multimedia, podrían permitir la ejecución remota de código(979902)  MS10-044: Vulnerabilidades en Microsoft Office Access ActiveX Controls podrían permitir la ejecución remota de código (982335)  MS10-055: Vulnerabilidad en códec multimedia Cinepak podría permitir la ejecución remota de código (982665)  MS10-059: Vulnerabilidades en la función de seguimiento para los servicios podrían permitir elevación de privilegios  MS10-060:. Vulnerabilidades en Microsoft NET Common Language Runtime y en Microsoft Silverlight de podrían permitir la ejecución remota de código  MS10-082: Vulnerabilidad en Windows Media Player, podría permitir la ejecución remota de código (2378111)  MS10-083: Una vulnerabilidad en la validación COM en el shell de Windows y WordPad, podría permitir la ejecución remota de código (2405882)  MS11-091: Vulnerabilidad en Microsoft Publisher podría permitir la ejecución remota de código  MS12-046: Vulnerabilidad en Visual Basic for Applications podría permitir la ejecución de código remoto (2707960)  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  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)  MS13-005: Vulnerabilidad en Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2778930) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.162 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2695962: Actualización para ActiveX en sus Kill Bits (2695962)  MS KB2269637: Carga insegura de librerías podría permitir ejecución remota de código  MS KB2719662: Vulnerabilidades en Gadgets podría permitir la ejecución de código remoto  MS07-023: Vulnerabilidad en Microsoft Excel  MS07-025: Código arbitrario puede llegar a ser ejecutado a través de Microsoft Office  MS07-036: Vulnerabilidad en Microsoft Excel  MS07-037: Vulnerabilidad en Microsoft Publisher podría permitir ejecución remota de código (936548)  MS08-014: Vulnerabilidades en Microsoft Excel podrían permitir la ejecución remota de código  MS08-015: Vulnerabilidad en Microsoft Outlook  MS08-026: Vulnerabilidad en Microsoft Word  MS08-027: Microsoft Publisher presenta múltiples vulnerabilidades que permite la ejecución de código remoto  MS08-043: Vulnerabilidad en Microsoft Excel  MS08-051: Vulnerabilidad en Microsoft PowerPoint  MS08-052: Vulnerabilidades en GDI+ podrían permitir la ejecución remota de código  MS08-055: Vulnerabilidad en Microsoft Office  MS08-057: Ejecución remota de código en múltiples métodos de Microsoft Excel  MS08-069: Ejecución remota de código sobre Microsoft XML Core Services (955218)  MS08-072: Vulnerabilidad en Microsoft Word  MS08-074: Microsoft Excel cuenta con múltiples métodos que permiten la ejecución de código remoto  MS09-009: Vulnerabilidades en Microsoft Office Excel podrían permitir ejecución remota de código  MS09-017: Microsoft Office PowerPoint presenta vulnerabilidades podrían permitir la ejecución de código remoto  MS09-021: Vulnerabilidades en Microsoft Office Excel podrían permitir la ejecución remota de código.  MS09-024: Código arbitrario puede llegar a ser ejecutado a través de Microsoft Office  MS09-027: Vulnerabilidades en Microsoft Office Word podrían permitir la ejecución remota de código  MS09-059: Vulnerabilidad en LSSAS (Local Security Authority Subsystem Servic) podría permitir una denegación de servicio  MS09-060: Vulnerabilidades en Controles ActiveX de Microsoft Active Template Library (ATL) para Microsoft Office podrían permitir la ejecución remota de código (973965)  MS09-067: Vulnerabilidades en Microsoft Office Excel podrían permitir la ejecución remota de código (972652)  MS10-001: OpenType Font Engine permite la ejecución de código remoto  MS10-017: Vulnerabilidades en Microsoft Office Excel podrían permitir la ejecución remota de código (980150)  MS10-019: Vulnerabilidades en Windows podrían permitir la ejecución de código (981210)  MS10-023: Vulnerabilidad en Microsoft Office Publisher podría permitir la ejecución remota de código  MS10-031: Vulnerabilidad en Microsoft Visual Basic para aplicaciones podría permitir la ejecución remota de código  MS10-033: Vulnerabilidades en la descompresión de archivos multimedia, podrían permitir la ejecución remota de código(979902)  MS10-036: Vulnerabilidad en la validación de COM en Microsoft Office podría permitir la ejecución remota de código (983235)  MS10-038: Vulnerabilidades en Microsoft Office Excel podrían permitir la ejecución remota de código(2027452)  MS10-044: Vulnerabilidades en Microsoft Office Access ActiveX Controls podrían permitir la ejecución remota de código (982335)  MS10-045: Vulnerabilidad en Microsoft Outlook  MS10-055: Vulnerabilidad en códec multimedia Cinepak podría permitir la ejecución remota de código (982665)  MS10-056: Vulnerabilidad en Microsoft Office Word podría permitir la ejecución remota de código (2269638)  MS10-059: Vulnerabilidades en la función de seguimiento para los servicios podrían permitir elevación de privilegios  MS10-064: Vulnerabilidad en Microsoft Office  MS10-074: Vulnerabilidad en Microsoft Foundation Classes podría permitir la ejecución remota de código  MS10-075: Vulnerabilidad en el servicio de Media Player Network Sharing puede permitir ejecución remota de código  MS10-076: Vulnerabilidad en el motor de fuentes OpenType que podría permitir la ejecución de código remotamente  MS10-079: Vulnerabilidades en Microsoft Word podrían permitir la ejecución remota de código (2293194)  MS10-080: Vulnerabilidades en Microsoft Excel podrían permitir la ejecución remota de código (2293211)  MS10-081: Vulnerabilidad en Windows en los controles de librería permita la ejecución remota de código  MS10-082: Vulnerabilidad en Windows Media Player, podría permitir la ejecución remota de código (2378111)  MS10-083: Una vulnerabilidad en la validación COM en el shell de Windows y WordPad, podría permitir la ejecución remota de código (2405882)  MS10-088: Vulnerabilidades en Microsoft PowerPoint podrían permitir la ejecución remota de código (2293386)  MS10-092: Vulnerabilidad en el programador de tareas (task scheduler) podría permitir la elevación de privilegios  MS10-096: Vulnerabilidad en Windows Address Book podría permitir la ejecución remota de código  MS10-100: Vulnerabilidad en la Interfaz del usuario podría permitir la elevación de privilegios  MS10-103: Microsoft Publisher podría permitir la ejecución código remoto  MS10-105:Vulnerabilidad en Microsoft Office  MS11-021: Vulnerabilidades en Microsoft Excel podrían permitir la ejecución remota de código (2489279)  MS11-022: Vulnerabilidades en Microsoft PowerPoint podrían permitir la ejecución remota de código (2489283)  MS11-036: Vulnerabilidades en Microsoft PowerPoint podrían permitir ejecutar código remoto (2545814)  MS11-038: Vulnerabilidades en OLE Automation podrían permitir ejecución de código remoto (2476490)  MS11-045: Vulnerabilidad en Microsoft Excel podría permitir ejecución de código remota (2537146)  MS11-072: Vulnerabilidades en Microsoft Excel podría permitir la ejecución remota de código (2587505)  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)  MS11-091: Vulnerabilidad en Microsoft Publisher podría permitir la ejecución remota de código  MS11-094: Una vulnerabilidad en Microsoft PowerPoint podrían permitir la ejecución remota de código  MS12-027: Vulnerabilidad en Windows Common Controls podría ocasionar ejecución de código remoto (2664258)  MS12-029: Vulnerabilidad en Microsoft Word podría ocasionar ejecución remota de código (2680352)  MS12-030: Vulnerabilidad en Microsoft Office podría ocasionar ejecución remota de código (2663830)  MS12-039: Vulnerabilidad en Lync podría permitir la ejecución de código remoto (2707956)  MS12-043: Vulnerabilidades en Microsoft XML Core Services podrían permitir la ejecución de código remoto (2722479)  MS12-046: Vulnerabilidad en Visual Basic for Applications podría permitir la ejecución de código remoto (2707960)  MS12-060: Vulnerabilidad en Windows Common Controls podría permitir la ejecución de código remoto (2720573)  MS12-064: Vulnerabilidad en Microsoft Word podría permitir la ejecución de código remoto (2742319)  MS12-076: Vulnerabilidad en Microsoft Office podría permitir la ejecución de código remoto (2720184)  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  MS12-079: Vulnerabili en Microsoft Word podría permitir la ejecución remota de código (2780642)  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)  MS13-005: Vulnerabilidad en Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2778930) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.171 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2695962: Actualización para ActiveX en sus Kill Bits (2695962)  MS KB2269637: Carga insegura de librerías podría permitir ejecución remota de código  MS KB2719662: Vulnerabilidades en Gadgets podría permitir la ejecución de código remoto  MS10-033: Vulnerabilidades en la descompresión de archivos multimedia, podrían permitir la ejecución remota de código(979902)  MS10-044: Vulnerabilidades en Microsoft Office Access ActiveX Controls podrían permitir la ejecución remota de código (982335)  MS10-055: Vulnerabilidad en códec multimedia Cinepak podría permitir la ejecución remota de código (982665)  MS10-059: Vulnerabilidades en la función de seguimiento para los servicios podrían permitir elevación de privilegios  MS10-082: Vulnerabilidad en Windows Media Player, podría permitir la ejecución remota de código (2378111)  MS10-083: Una vulnerabilidad en la validación COM en el shell de Windows y WordPad, podría permitir la ejecución remota de código (2405882)  MS11-025: Vulnerabilidad en la librería Microsoft Foundation Class (MFC), podría permitir la ejecución remota de código (2500212)  MS11-091: Vulnerabilidad en Microsoft Publisher podría permitir la ejecución remota de código  MS12-034: Actualizaciones de Seguridad para Microsoft Office, Windows, .NET Framework, y Silverlight (2681578)  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  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)  MS13-005: Vulnerabilidad en Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2778930) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.187 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2695962: Actualización para ActiveX en sus Kill Bits (2695962)  MS KB2269637: Carga insegura de librerías podría permitir ejecución remota de código  MS KB2719662: Vulnerabilidades en Gadgets podría permitir la ejecución de código remoto  MS10-033: Vulnerabilidades en la descompresión de archivos multimedia, podrían permitir la ejecución remota de código(979902)  MS10-044: Vulnerabilidades en Microsoft Office Access ActiveX Controls podrían permitir la ejecución remota de código (982335)  MS10-055: Vulnerabilidad en códec multimedia Cinepak podría permitir la ejecución remota de código (982665)  MS10-059: Vulnerabilidades en la función de seguimiento para los servicios podrían permitir elevación de privilegios  MS10-060:. Vulnerabilidades en Microsoft NET Common Language Runtime y en Microsoft Silverlight de podrían permitir la ejecución remota de código  MS10-082: Vulnerabilidad en Windows Media Player, podría permitir la ejecución remota de código (2378111)  MS10-083: Una vulnerabilidad en la validación COM en el shell de Windows y WordPad, podría permitir la ejecución remota de código (2405882)  MS11-091: Vulnerabilidad en Microsoft Publisher podría permitir la ejecución remota de código  MS12-039: Vulnerabilidad en Lync podría permitir la ejecución de código remoto (2707956)  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  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)  MS13-005: Vulnerabilidad en Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2778930) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.192 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2695962: Actualización para ActiveX en sus Kill Bits (2695962)  MS KB2269637: Carga insegura de librerías podría permitir ejecución remota de código  MS KB2719662: Vulnerabilidades en Gadgets podría permitir la ejecución de código remoto  MS09-059: Vulnerabilidad en LSSAS (Local Security Authority Subsystem Servic) podría permitir una denegación de servicio  MS09-060: Vulnerabilidades en Controles ActiveX de Microsoft Active Template Library (ATL) para Microsoft Office podrían permitir la ejecución remota de código (973965)  MS10-033: Vulnerabilidades en la descompresión de archivos multimedia, podrían permitir la ejecución remota de código(979902)  MS10-044: Vulnerabilidades en Microsoft Office Access ActiveX Controls podrían permitir la ejecución remota de código (982335)  MS10-055: Vulnerabilidad en códec multimedia Cinepak podría permitir la ejecución remota de código (982665)  MS10-059: Vulnerabilidades en la función de seguimiento para los servicios podrían permitir elevación de privilegios  MS10-060:. Vulnerabilidades en Microsoft NET Common Language Runtime y en Microsoft Silverlight de podrían permitir la ejecución remota de código  MS10-082: Vulnerabilidad en Windows Media Player, podría permitir la ejecución remota de código (2378111)  MS10-083: Una vulnerabilidad en la validación COM en el shell de Windows y WordPad, podría permitir la ejecución remota de código (2405882)  MS11-091: Vulnerabilidad en Microsoft Publisher podría permitir la ejecución remota de código  MS12-039: Vulnerabilidad en Lync podría permitir la ejecución de código remoto (2707956)  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  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)  MS13-005: Vulnerabilidad en Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2778930) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.209 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2695962: Actualización para ActiveX en sus Kill Bits (2695962)  MS KB2269637: Carga insegura de librerías podría permitir ejecución remota de código  MS KB2719662: Vulnerabilidades en Gadgets podría permitir la ejecución de código remoto  MS09-035: Múltiples Vulnerabilidades en Visual Studio Active Template Library permiten de manera remota la ejecución de código (969706)  MS10-012: Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código  MS10-033: Vulnerabilidades en la descompresión de archivos multimedia, podrían permitir la ejecución remota de código(979902)  MS10-044: Vulnerabilidades en Microsoft Office Access ActiveX Controls podrían permitir la ejecución remota de código (982335)  MS10-055: Vulnerabilidad en códec multimedia Cinepak podría permitir la ejecución remota de código (982665)  MS10-059: Vulnerabilidades en la función de seguimiento para los servicios podrían permitir elevación de privilegios  MS10-060:. Vulnerabilidades en Microsoft NET Common Language Runtime y en Microsoft Silverlight de podrían permitir la ejecución remota de código  MS10-082: Vulnerabilidad en Windows Media Player, podría permitir la ejecución remota de código (2378111)  MS10-083: Una vulnerabilidad en la validación COM en el shell de Windows y WordPad, podría permitir la ejecución remota de código (2405882)  MS11-025: Vulnerabilidad en la librería Microsoft Foundation Class (MFC), podría permitir la ejecución remota de código (2500212)  MS11-091: Vulnerabilidad en Microsoft Publisher podría permitir la ejecución remota de código  MS12-039: Vulnerabilidad en Lync podría permitir la ejecución de código remoto (2707956)  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  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)  MS13-005: Vulnerabilidad en Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2778930) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.221 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2695962: Actualización para ActiveX en sus Kill Bits (2695962)  MS KB2269637: Carga insegura de librerías podría permitir ejecución remota de código  MS KB2719662: Vulnerabilidades en Gadgets podría permitir la ejecución de código remoto  MS09-059: Vulnerabilidad en LSSAS (Local Security Authority Subsystem Servic) podría permitir una denegación de servicio  MS09-060: Vulnerabilidades en Controles ActiveX de Microsoft Active Template Library (ATL) para Microsoft Office podrían permitir la ejecución remota de código (973965)  MS10-033: Vulnerabilidades en la descompresión de archivos multimedia, podrían permitir la ejecución remota de código(979902)  MS10-044: Vulnerabilidades en Microsoft Office Access ActiveX Controls podrían permitir la ejecución remota de código (982335)  MS10-055: Vulnerabilidad en códec multimedia Cinepak podría permitir la ejecución remota de código (982665)  MS10-059: Vulnerabilidades en la función de seguimiento para los servicios podrían permitir elevación de privilegios  MS10-082: Vulnerabilidad en Windows Media Player, podría permitir la ejecución remota de código (2378111)  MS10-083: Una vulnerabilidad en la validación COM en el shell de Windows y WordPad, podría permitir la ejecución remota de código (2405882)  MS12-034: Actualizaciones de Seguridad para Microsoft Office, Windows, .NET Framework, y Silverlight (2681578)  MS12-039: Vulnerabilidad en Lync podría permitir la ejecución de código remoto (2707956)  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  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)  MS13-005: Vulnerabilidad en Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2778930) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.234 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2695962: Actualización para ActiveX en sus Kill Bits (2695962)  MS KB2269637: Carga insegura de librerías podría permitir ejecución remota de código  MS KB2719662: Vulnerabilidades en Gadgets podría permitir la ejecución de código remoto  MS09-043: Microsoft Office Web Components Control presenta una vulnerabilidad de ejecución de código remoto  MS09-043: Microsoft Office Web Components presenta una vulnerabilidad que permite la ejecución de código remoto  MS10-033: Vulnerabilidades en la descompresión de archivos multimedia, podrían permitir la ejecución remota de código(979902)  MS10-055: Vulnerabilidad en códec multimedia Cinepak podría permitir la ejecución remota de código (982665)  MS10-059: Vulnerabilidades en la función de seguimiento para los servicios podrían permitir elevación de privilegios  MS10-060:. Vulnerabilidades en Microsoft NET Common Language Runtime y en Microsoft Silverlight de podrían permitir la ejecución remota de código  MS10-079: Vulnerabilidades en Microsoft Word podrían permitir la ejecución remota de código (2293194)  MS10-082: Vulnerabilidad en Windows Media Player, podría permitir la ejecución remota de código (2378111)  MS10-083: Una vulnerabilidad en la validación COM en el shell de Windows y WordPad, podría permitir la ejecución remota de código (2405882)  MS10-087: Microsoft Office puede permitir la ejecución de código remoto  MS10-103: Microsoft Publisher podría permitir la ejecución código remoto  MS10-105:Vulnerabilidad en Microsoft Office  MS11-021: Vulnerabilidades en Microsoft Excel podrían permitir la ejecución remota de código (2489279)  MS11-022: Vulnerabilidades en Microsoft PowerPoint podrían permitir la ejecución remota de código (2489283)  MS11-045: Vulnerabilidad en Microsoft Excel podría permitir ejecución de código remota (2537146)  MS11-072: Vulnerabilidades en Microsoft Excel podría permitir la ejecución remota de código (2587505)  MS11-073: Vulnerabilidades en Microsoft Office podría permitir ejecución de código remoto (2587634)  MS11-089: Una vulnerabilidad en Microsoft Office podría permitir la ejecución remota de código  MS11-094: Una vulnerabilidad en Microsoft PowerPoint podrían permitir la ejecución remota de código  MS12-015: Vulnerabilidades en Microsoft Visio Viewer 2010 podrían permitir ejecución remota de código (2663510)  MS12-025: Vulnerabilidad en .NET Framework podría ocasionar ejecución remota de código (2671605)  MS12-027: Vulnerabilidad en Windows Common Controls podría ocasionar ejecución de código remoto (2664258)  MS12-030: Vulnerabilidad en Microsoft Office podría ocasionar ejecución remota de código (2663830)  MS12-031: Vulnerabilidad en Microsoft Visio Viewer 2010 podría ocasionar ejecución remota de código (2597981)  MS12-039: Vulnerabilidad en Lync podría permitir la ejecución de código remoto (2707956)  MS12-046: Vulnerabilidad en Visual Basic for Applications podría permitir la ejecución de código remoto (2707960)  MS12-059: Microsoft Visio y Visio Viewer permite la ejecución de código remoto (2733918)  MS12-060: Vulnerabilidad en Windows Common Controls podría permitir la ejecución de código remoto (2720573)  MS12-074: Vulnerabilidad en .NET Framework podría permitir la ejecución de código remoto (2745030)  MS12-076: Vulnerabilidad en Microsoft Office podría permitir la ejecución de código remoto (2720184)  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  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)  MS13-005: Vulnerabilidad en Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2778930) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.238 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2695962: Actualización para ActiveX en sus Kill Bits (2695962)  MS KB2269637: Carga insegura de librerías podría permitir ejecución remota de código  MS KB2719662: Vulnerabilidades en Gadgets podría permitir la ejecución de código remoto  MS09-043: Microsoft Office Web Components Control presenta una vulnerabilidad de ejecución de código remoto  MS09-043: Microsoft Office Web Components presenta una vulnerabilidad que permite la ejecución de código remoto  MS10-033: Vulnerabilidades en la descompresión de archivos multimedia, podrían permitir la ejecución remota de código(979902)  MS10-055: Vulnerabilidad en códec multimedia Cinepak podría permitir la ejecución remota de código (982665)  MS10-059: Vulnerabilidades en la función de seguimiento para los servicios podrían permitir elevación de privilegios  MS10-060:. Vulnerabilidades en Microsoft NET Common Language Runtime y en Microsoft Silverlight de podrían permitir la ejecución remota de código  MS10-082: Vulnerabilidad en Windows Media Player, podría permitir la ejecución remota de código (2378111)  MS10-083: Una vulnerabilidad en la validación COM en el shell de Windows y WordPad, podría permitir la ejecución remota de código (2405882)  MS10-087: Microsoft Office puede permitir la ejecución de código remoto  MS10-105:Vulnerabilidad en Microsoft Office  MS11-021: Vulnerabilidades en Microsoft Excel podrían permitir la ejecución remota de código (2489279)  MS11-022: Vulnerabilidades en Microsoft PowerPoint podrían permitir la ejecución remota de código (2489283)  MS11-025: Vulnerabilidad en la librería Microsoft Foundation Class (MFC), podría permitir la ejecución remota de código (2500212)  MS11-045: Vulnerabilidad en Microsoft Excel podría permitir ejecución de código remota (2537146)  MS11-072: Vulnerabilidades en Microsoft Excel podría permitir la ejecución remota de código (2587505)  MS11-073: Vulnerabilidades en Microsoft Office podría permitir ejecución de código remoto (2587634)  MS11-089: Una vulnerabilidad en Microsoft Office podría permitir la ejecución remota de código  MS11-094: Una vulnerabilidad en Microsoft PowerPoint podrían permitir la ejecución remota de código  MS12-015: Vulnerabilidades en Microsoft Visio Viewer 2010 podrían permitir ejecución remota de código (2663510)  MS12-025: Vulnerabilidad en .NET Framework podría ocasionar ejecución remota de código (2671605)  MS12-027: Vulnerabilidad en Windows Common Controls podría ocasionar ejecución de código remoto (2664258)  MS12-030: Vulnerabilidad en Microsoft Office podría ocasionar ejecución remota de código (2663830)  MS12-039: Vulnerabilidad en Lync podría permitir la ejecución de código remoto (2707956)  MS12-046: Vulnerabilidad en Visual Basic for Applications podría permitir la ejecución de código remoto (2707960)  MS12-059: Microsoft Visio y Visio Viewer permite la ejecución de código remoto (2733918)  MS12-060: Vulnerabilidad en Windows Common Controls podría permitir la ejecución de código remoto (2720573)  MS12-074: Vulnerabilidad en .NET Framework podría permitir la ejecución de código remoto (2745030)  MS12-076: Vulnerabilidad en Microsoft Office podría permitir la ejecución de código remoto (2720184)  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  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)  MS13-005: Vulnerabilidad en Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2778930) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.239 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2695962: Actualización para ActiveX en sus Kill Bits (2695962)  MS KB2269637: Carga insegura de librerías podría permitir ejecución remota de código  MS KB2719662: Vulnerabilidades en Gadgets podría permitir la ejecución de código remoto  MS09-059: Vulnerabilidad en LSSAS (Local Security Authority Subsystem Servic) podría permitir una denegación de servicio  MS10-012: Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código  MS10-033: Vulnerabilidades en la descompresión de archivos multimedia, podrían permitir la ejecución remota de código(979902)  MS10-055: Vulnerabilidad en códec multimedia Cinepak podría permitir la ejecución remota de código (982665)  MS10-059: Vulnerabilidades en la función de seguimiento para los servicios podrían permitir elevación de privilegios  MS10-060:. Vulnerabilidades en Microsoft NET Common Language Runtime y en Microsoft Silverlight de podrían permitir la ejecución remota de código  MS10-082: Vulnerabilidad en Windows Media Player, podría permitir la ejecución remota de código (2378111)  MS10-083: Una vulnerabilidad en la validación COM en el shell de Windows y WordPad, podría permitir la ejecución remota de código (2405882)  MS10-087: Microsoft Office puede permitir la ejecución de código remoto  MS10-105:Vulnerabilidad en Microsoft Office  MS11-022: Vulnerabilidades en Microsoft PowerPoint podrían permitir la ejecución remota de código (2489283)  MS11-025: Vulnerabilidad en la librería Microsoft Foundation Class (MFC), podría permitir la ejecución remota de código (2500212)  MS11-073: Vulnerabilidades en Microsoft Office podría permitir ejecución de código remoto (2587634)  MS11-089: Una vulnerabilidad en Microsoft Office podría permitir la ejecución remota de código  MS11-094: Una vulnerabilidad en Microsoft PowerPoint podrían permitir la ejecución remota de código  MS12-015: Vulnerabilidades en Microsoft Visio Viewer 2010 podrían permitir ejecución remota de código (2663510)  MS12-025: Vulnerabilidad en .NET Framework podría ocasionar ejecución remota de código (2671605)  MS12-027: Vulnerabilidad en Windows Common Controls podría ocasionar ejecución de código remoto (2664258)  MS12-031: Vulnerabilidad en Microsoft Visio Viewer 2010 podría ocasionar ejecución remota de código (2597981)  MS12-039: Vulnerabilidad en Lync podría permitir la ejecución de código remoto (2707956)  MS12-046: Vulnerabilidad en Visual Basic for Applications podría permitir la ejecución de código remoto (2707960)  MS12-059: Microsoft Visio y Visio Viewer permite la ejecución de código remoto (2733918)  MS12-060: Vulnerabilidad en Windows Common Controls podría permitir la ejecución de código remoto (2720573)  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: Vulnerabilidad 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)  MS13-005: Vulnerabilidad en Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2778930) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.246 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS11-091: Vulnerabilidad en Microsoft Publisher podría permitir la ejecución remota de código | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.251 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2695962: Actualización para ActiveX en sus Kill Bits (2695962)  MS KB2269637: Carga insegura de librerías podría permitir ejecución remota de código  MS KB2719662: Vulnerabilidades en Gadgets podría permitir la ejecución de código remoto  MS08-070: Vulnerabilidades en controles de Visual Basic 6.0 ActiveX pueden permitir la ejecución remota de código  MS10-033: Vulnerabilidades en la descompresión de archivos multimedia, podrían permitir la ejecución remota de código(979902)  MS10-044: Vulnerabilidades en Microsoft Office Access ActiveX Controls podrían permitir la ejecución remota de código (982335)  MS10-055: Vulnerabilidad en códec multimedia Cinepak podría permitir la ejecución remota de código (982665)  MS10-059: Vulnerabilidades en la función de seguimiento para los servicios podrían permitir elevación de privilegios  MS10-082: Vulnerabilidad en Windows Media Player, podría permitir la ejecución remota de código (2378111)  MS10-083: Una vulnerabilidad en la validación COM en el shell de Windows y WordPad, podría permitir la ejecución remota de código (2405882)  MS11-091: Vulnerabilidad en Microsoft Publisher podría permitir la ejecución remota de código  MS12-039: Vulnerabilidad en Lync podría permitir la ejecución de código remoto (2707956)  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  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)  MS13-005: Vulnerabilidad en Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2778930) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.252 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2695962: Actualización para ActiveX en sus Kill Bits (2695962)  MS KB2269637: Carga insegura de librerías podría permitir ejecución remota de código  MS KB2719662: Vulnerabilidades en Gadgets podría permitir la ejecución de código remoto  MS09-035: Múltiples Vulnerabilidades en Visual Studio Active Template Library permiten de manera remota la ejecución de código (969706)  MS10-033: Vulnerabilidades en la descompresión de archivos multimedia, podrían permitir la ejecución remota de código(979902)  MS10-044: Vulnerabilidades en Microsoft Office Access ActiveX Controls podrían permitir la ejecución remota de código (982335)  MS10-055: Vulnerabilidad en códec multimedia Cinepak podría permitir la ejecución remota de código (982665)  MS10-059: Vulnerabilidades en la función de seguimiento para los servicios podrían permitir elevación de privilegios  MS10-060:. Vulnerabilidades en Microsoft NET Common Language Runtime y en Microsoft Silverlight de podrían permitir la ejecución remota de código  MS10-082: Vulnerabilidad en Windows Media Player, podría permitir la ejecución remota de código (2378111)  MS10-083: Una vulnerabilidad en la validación COM en el shell de Windows y WordPad, podría permitir la ejecución remota de código (2405882)  MS11-025: Vulnerabilidad en la librería Microsoft Foundation Class (MFC), podría permitir la ejecución remota de código (2500212)  MS12-039: Vulnerabilidad en Lync podría permitir la ejecución de código remoto (2707956)  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  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)  MS13-005: Vulnerabilidad en Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2778930) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Adobe Acrobat Reader < 10.1.3 / 9.5.1 Múltiples Vulnerabilidades (APSB12-08)**

|  |
| --- |
| IP |
| 99.40.16.156 |
| 99.40.16.138 |
| 99.40.16.137 |

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

**Adobe Flash Player <= 10.3.183.19 / 11.3.300.256 Múltiples Vulnerabilidades (APSB12-14)**

|  |  |
| --- | --- |
| IP | |
| 99.40.16.252 | 99.40.16.192 |
| 99.40.16.251 | 99.40.16.187 |
| 99.40.16.246 | 99.40.16.171 |
| 99.40.16.239 | 99.40.16.162 |
| 99.40.16.238 | 99.40.16.156 |
| 99.40.16.234 | 99.40.16.145 |
| 99.40.16.221 | 99.40.16.138 |
| 99.40.16.209 | 99.40.16.137 |

|  |  |  |
| --- | --- | --- |
| **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 Windows es menor a la versión 10.3.183.19 u 11.x. Dichas versiones anteriores se ven afectadas por múltiples problemas de seguridad:  - Múltiples corrupciones de memoria. (CVE-2012-2034,  CVE-2012-2037)  - Desbordamiento de búfer podría permitir la ejecución de código. (CVE-2012-2035) (CVE-2012-2036)  - Un problema de evasión de vulnerabilidades podría ocacionar fuga de información. (CVE-2012-2038)  - Un problema de una referencia nula podría permitir la ejecución de código. (CVE-2012-2039) |
| Solución: | | |
| Actualizar Adobe Flash Player a la versión 10.3.183.20 / 11.3.300.257 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 | |
| 99.40.16.252 | 99.40.16.187 |
| 99.40.16.251 | 99.40.16.171 |
| 99.40.16.239 | 99.40.16.162 |
| 99.40.16.238 | 99.40.16.156 |
| 99.40.16.234 | 99.40.16.145 |
| 99.40.16.221 | 99.40.16.138 |
| 99.40.16.209 | 99.40.16.137 |
| 99.40.16.192 | 99.40.16.187 |

|  |  |  |
| --- | --- | --- |
| **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 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 posterior. 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** | | | |
| 99.40.16.252 | 99.40.16.238 | 99.40.16.192 | 99.40.16.162 |
| 99.40.16.251 | 99.40.16.234 | 99.40.16.187 | 99.40.16.156 |
| 99.40.16.250 | 99.40.16.221 | 99.40.16.182 | 99.40.16.151 |
| 99.40.16.246 | 99.40.16.214 | 99.40.16.180 | 99.40.16.145 |
| 99.40.16.242 | 99.40.16.209 | 99.40.16.176 | 99.40.16.138 |
| 99.40.16.239 | 99.40.16.202 | 99.40.16.171 | 99.40.16.137 |

|  |  |  |
| --- | --- | --- |
| **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 le 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 Office Service Pack desactualizado**

|  |
| --- |
| **IP** |
| 99.40.16.246 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 7.1 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:C) | El equipo remoto Microsoft Windows se encuentra ejecutando una version de Microsoft Silverligth que es afectada por múltiples vulnerabilidades:  - Una corrupción de memoria existerelacionada con un control de popup y unpropiedad llamada "DependencyProperty" (CVE-2011-1844).  - Múltiples problemas de memoria existen en la implementación del control 'DataGrid' (CVE-2011-1845). |
| Solución: | | |
| Actualizar a Silverlight 4.0.60310.0 o superior.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

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

|  |  |
| --- | --- |
| **IP** | |
| 99.40.16.252 | 99.40.16.187 |
| 99.40.16.246 | 99.40.16.171 |
| 99.40.16.239 | 99.40.16.156 |
| 99.40.16.238 | 99.40.16.145 |
| 99.40.16.234 | 99.40.16.138 |
| 99.40.16.137 | 99.40.16.209 |
| 99.40.16.221 | 99.40.16.192 |

|  |  |  |
| --- | --- | --- |
| **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) | 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** | |
| 99.40.16.252 | 99.40.16.187 |
| 99.40.16.251 | 99.40.16.171 |
| 99.40.16.239 | 99.40.16.162 |
| 99.40.16.238 | 99.40.16.156 |
| 99.40.16.234 | 99.40.16.145 |
| 99.40.16.221 | 99.40.16.138 |
| 99.40.16.192 | 99.40.16.137 |

|  |  |  |
| --- | --- | --- |
| **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** |
| 99.40.16.239 |
| 99.40.16.209 |
| 99.40.16.187 |
| 99.40.16.171 |
| 99.40.16.145 |
| 99.40.16.138 |
| 99.40.16.137 |

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

### Vulnerabilidades de prioridad Media para CLIENTE99.40.16.0

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.137 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Medio / CVSS Base Score : 6.4  (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2647518: Actualización para ActiveX Kill Bits (2647518)  MS KB2728973: Certificados digitales no autorizados podrían permitir la suplantación de identidad  MS KB982316: Elevación de privilegios a través de evadir Windows Service Isolation  MS10-041: Vulnerabilidad en Microsoft .Net Framework que podría permitir falsificaciones (981343)  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) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.138 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Medio / CVSS Base Score : 6.4  (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2647518: Actualización para ActiveX Kill Bits (2647518)  MS KB2728973: Certificados digitales no autorizados podrían permitir la suplantación de identidad  MS KB982316: Elevación de privilegios a través de evadir Windows Service Isolation  MS10-041: Vulnerabilidad en Microsoft .Net Framework que podría permitir falsificaciones (981343)  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) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.145 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Medio / CVSS Base Score : 6.4  (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2647518: Actualización para ActiveX Kill Bits (2647518)  MS KB2728973: Certificados digitales no autorizados podrían permitir la suplantación de identidad  MS KB982316: Elevación de privilegios a través de evadir Windows Service Isolation  MS10-041: Vulnerabilidad en Microsoft .Net Framework que podría permitir falsificaciones (981343)  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) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.156 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Medio / CVSS Base Score : 6.4  (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2647518: Actualización para ActiveX Kill Bits (2647518)  MS KB2728973: Certificados digitales no autorizados podrían permitir la suplantación de identidad  MS KB982316: Elevación de privilegios a través de evadir Windows Service Isolation  MS09-056: Vulnerabilidades en Windows CryptoAPI podrían permitir suplantación de identidad (spoofing)  MS10-041: Vulnerabilidad en Microsoft .Net Framework que podría permitir falsificaciones (981343)  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) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.162 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Medio / CVSS Base Score : 6.4  (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2647518: Actualización para ActiveX Kill Bits (2647518)  MS KB2728973: Certificados digitales no autorizados podrían permitir la suplantación de identidad  MS KB982316: Elevación de privilegios a través de evadir Windows Service Isolation  MS09-056: Vulnerabilidades en Windows CryptoAPI podrían permitir suplantación de identidad (spoofing)  MS10-041: Vulnerabilidad en Microsoft .Net Framework que podría permitir falsificaciones (981343)  MS12-050: Vulnerabilidades en SharePoint podrían permitir la elevación de privilegios (2695502)  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) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.171 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Medio / CVSS Base Score : 6.4  (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2647518: Actualización para ActiveX Kill Bits (2647518)  MS KB2728973: Certificados digitales no autorizados podrían permitir la suplantación de identidad  MS KB982316: Elevación de privilegios a través de evadir Windows Service Isolation  MS10-041: Vulnerabilidad en Microsoft .Net Framework que podría permitir falsificaciones (981343)  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) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.187 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Medio / CVSS Base Score : 6.4  (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2647518: Actualización para ActiveX Kill Bits (2647518)  MS KB2728973: Certificados digitales no autorizados podrían permitir la suplantación de identidad  MS KB982316: Elevación de privilegios a través de evadir Windows Service Isolation  MS10-041: Vulnerabilidad en Microsoft .Net Framework que podría permitir falsificaciones (981343)  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) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.192 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Medio / CVSS Base Score : 6.4  (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2647518: Actualización para ActiveX Kill Bits (2647518)  MS KB2728973: Certificados digitales no autorizados podrían permitir la suplantación de identidad  MS KB982316: Elevación de privilegios a través de evadir Windows Service Isolation  MS09-056: Vulnerabilidades en Windows CryptoAPI podrían permitir suplantación de identidad (spoofing)  MS10-041: Vulnerabilidad en Microsoft .Net Framework que podría permitir falsificaciones (981343)  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) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.209 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Medio / CVSS Base Score : 6.4  (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2647518: Actualización para ActiveX Kill Bits (2647518)  MS KB2728973: Certificados digitales no autorizados podrían permitir la suplantación de identidad  MS KB982316: Elevación de privilegios a través de evadir Windows Service Isolation  MS10-041: Vulnerabilidad en Microsoft .Net Framework que podría permitir falsificaciones (981343)  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) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.221 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Medio / CVSS Base Score : 6.4  (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2647518: Actualización para ActiveX Kill Bits (2647518)  MS KB2728973: Certificados digitales no autorizados podrían permitir la suplantación de identidad  MS KB982316: Elevación de privilegios a través de evadir Windows Service Isolation  MS09-056: Vulnerabilidades en Windows CryptoAPI podrían permitir suplantación de identidad (spoofing)  MS10-041: Vulnerabilidad en Microsoft .Net Framework que podría permitir falsificaciones (981343)  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) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.234 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Medio / CVSS Base Score : 6.4  (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2647518: Actualización para ActiveX Kill Bits (2647518)  MS KB2728973: Certificados digitales no autorizados podrían permitir la suplantación de identidad  MS KB982316: Elevación de privilegios a través de evadir Windows Service Isolation  MS10-041: Vulnerabilidad en Microsoft .Net Framework que podría permitir falsificaciones (981343)  MS11-074: Vulnerabilidad en Microsoft SharePoint podría permitir elevación de privilegios (2451858)  MS12-050: Vulnerabilidades en SharePoint podrían permitir la elevación de privilegios (2695502)  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) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.238 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Medio / CVSS Base Score : 6.4  (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2647518: Actualización para ActiveX Kill Bits (2647518)  MS KB2728973: Certificados digitales no autorizados podrían permitir la suplantación de identidad  MS KB982316: Elevación de privilegios a través de evadir Windows Service Isolation  MS10-041: Vulnerabilidad en Microsoft .Net Framework que podría permitir falsificaciones (981343)  MS11-074: Vulnerabilidad en Microsoft SharePoint podría permitir elevación de privilegios (2451858)  MS12-050: Vulnerabilidades en SharePoint podrían permitir la elevación de privilegios (2695502)  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) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.239 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Medio / CVSS Base Score : 6.4  (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2647518: Actualización para ActiveX Kill Bits (2647518)  MS KB2728973: Certificados digitales no autorizados podrían permitir la suplantación de identidad  MS KB982316: Elevación de privilegios a través de evadir Windows Service Isolation  MS09-056: Vulnerabilidades en Windows CryptoAPI podrían permitir suplantación de identidad (spoofing)  MS10-041: Vulnerabilidad en Microsoft .Net Framework que podría permitir falsificaciones (981343)  MS11-074: Vulnerabilidad en Microsoft SharePoint podría permitir elevación de privilegios (2451858)  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) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.251 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Medio / CVSS Base Score : 6.4  (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2647518: Actualización para ActiveX Kill Bits (2647518)  MS KB2728973: Certificados digitales no autorizados podrían permitir la suplantación de identidad  MS KB982316: Elevación de privilegios a través de evadir Windows Service Isolation  MS10-041: Vulnerabilidad en Microsoft .Net Framework que podría permitir falsificaciones (981343)  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) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.252 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Medio / CVSS Base Score : 6.4  (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2647518: Actualización para ActiveX Kill Bits (2647518)  MS KB2728973: Certificados digitales no autorizados podrían permitir la suplantación de identidad  MS KB982316: Elevación de privilegios a través de evadir Windows Service Isolation  MS10-041: Vulnerabilidad en Microsoft .Net Framework que podría permitir falsificaciones (981343)  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) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Adobe Flash Player < 10.3.181.22 Cross-Site Scripting (XSS) (APSB11-13)**

|  |  |  |  |
| --- | --- | --- | --- |
| **IP** | | | |
| 99.40.16.252 | 99.40.16.238 | 99.40.16.192 | 99.40.16.156 |
| 99.40.16.251 | 99.40.16.234 | 99.40.16.187 | 99.40.16.145 |
| 99.40.16.246 | 99.40.16.221 | 99.40.16.171 | 99.40.16.138 |
| 99.40.16.239 | 99.40.16.209 | 99.40.16.162 | 99.40.16.137 |

|  |  |  |
| --- | --- | --- |
| **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) | Una vulnerabilidad de cross-site scripting existe en versiones de Flash Player menores a 10.3.181.22 (10.3.181.23 para ActiveX).  Un atacante podría aprovechar este problema para inyectar y ejecutar código arbitrario HTML y código script en el navegador del usuario. |
| Solución: | | |
| Actualizar a la versión más reciente de Adobe Flash 10.3.181.22 (10.3.181.23 en ActiveX) o superior.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Citrix XenApp Online Plug-in / Vulnerabilidad de suplantación de identidad (MiTM) a través de certificados especialmente diseñados**

|  |  |  |
| --- | --- | --- |
| **IP** | | |
| 99.40.16.252 | 99.40.16.221 | 99.40.16.162 |
| 99.40.16.251 | 99.40.16.209 | 99.40.16.156 |
| 99.40.16.239 | 99.40.16.192 | 99.40.16.145 |
| 99.40.16.238 | 99.40.16.187 | 99.40.16.138 |
| 99.40.16.234 | 99.40.16.171 | 99.40.16.137 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **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 trafico 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. | | |

**Symantec pcAnywhere vulnerabilidad en archivos CHF podría permitir una denegación de servicio**

|  |  |  |  |
| --- | --- | --- | --- |
| **IP** | | | |
| 99.40.16.252 | 99.40.16.238 | 99.40.16.192 | 99.40.16.156 |
| 99.40.16.251 | 99.40.16.234 | 99.40.16.187 | 99.40.16.145 |
| 99.40.16.246 | 99.40.16.221 | 99.40.16.171 | 99.40.16.138 |
| 99.40.16.239 | 99.40.16.209 | 99.40.16.162 | 99.40.16.137 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Media**  Media / 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** | | |
| 99.40.16.246 | 99.40.16.202 |
| 99.40.16.242 | 99.40.16.192 |
| 99.40.16.239 | 99.40.16.180 |
| 99.40.16.238 | 99.40.16.156 |
| 99.40.16.214 | 99.40.16.133 |
| 99.40.16.209 | 99.40.16.124 |

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

### Vulnerabilidades de prioridad Baja para CLIENTE99.40.16.0

**Almacenamiento de credenciales en memoria**

|  |  |  |  |
| --- | --- | --- | --- |
| **IP** | | | |
| 99.40.16.252 | 99.40.16.238 | 99.40.16.192 | 99.40.16.156 |
| 99.40.16.251 | 99.40.16.234 | 99.40.16.187 | 99.40.16.145 |
| 99.40.16.246 | 99.40.16.221 | 99.40.16.171 | 99.40.16.138 |
| 99.40.16.239 | 99.40.16.209 | 99.40.16.162 | 99.40.16.137 |

|  |  |  |
| --- | --- | --- |
| **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** | |
| 99.40.16.246 | 99.40.16.202 |
| 99.40.16.242 | 99.40.16.192 |
| 99.40.16.239 | 99.40.16.180 |
| 99.40.16.238 | 99.40.16.156 |
| 99.40.16.214 | 99.40.16.133 |
| 99.40.16.209 | 99.40.16.124 |

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

**Nessus UDP scanner**

|  |
| --- |
| **IP** |
| 99.40.16.61 |
| 99.40.16.250 |
| 99.40.16.182 |
| 99.40.16.180 |
| 99.40.16.176 |
| 99.40.16.151 |
| 99.40.16.102 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Baja** | 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 | | |

## Sección E. Recomendaciones

## Tecnología

Durante la realización del análisis de vulnerabilidades del mes de enero de 2013, se lograron identificar vulnerabilidades de nivel Alto, Medio y Bajo. Las vulnerabilidades afectan tanto a sistemas operativos como a las aplicaciones encontradas en los mismos.

La mayoría de las vulnerabilidades descubiertas pueden remediarse a través de las siguientes acciones:

* Instalación de parches y actualizaciones más recientes en aplicaciones, equipos y sistemas operativos.
* Determinar los parámetros necesarios para evitar una mala configuración o configuración por defecto en equipos.

Es importante mencionar que las mejores prácticas nos indican que antes de poder instalar un parche de seguridad o fortalecer cualquier servicio o sistema, los cambios deben ser verificados en ambientes de desarrollo para la validación del funcionamiento. Después de esto ya deben ser aplicados a los sistemas en producción. También antes de instalar cualquier actualización es importante la revisión de las políticas de seguridad de la organización, esto para la validación de los cambios correspondiente.

Dar prioridad a los equipos que muestran vulnerabilidades de tipo ALTA, MEDIA y BAJA en el mediano plazo, llevando a cabo las siguientes recomendaciones:

* Aplicar los parches correspondientes a sistemas operativos y aplicaciones contenidas en los mismos.
* Deshabilitar servicios no seguros en caso de no ser necesarios, o en su defecto manejar servicios alternativos que manejen cifrado de las comunicaciones.

## Procesos

* Crear un procedimiento que evalúe los sistemas operativos a utilizar y realice pruebas de compatibilidad con actualizaciones para mantener una configuración base (security baseline) que permita al servidor contar con una seguridad mínima aceptable.
* Ejecutar periódicamente pruebas de penetración para descubrir nuevos huecos de seguridad en las aplicaciones.
* Establecer una política de actualización de aplicaciones en equipos y servidores.
* Establecer y/o difundir y/o auditar una política de contraseñas para evitar contraseñas débiles, por defecto o en blanco.