**Segmento 99.40.16.0**

### 

### Vulnerabilidades de prioridad Alta para Administración Local De Recaudación De Guadalajara Centro

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.16.110 |

|  |  |  |
| --- | --- | --- |
| **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:**  MS11-048: Vulnerabilidad en SMB Server podría ocasionar una denegación de servicio (2536275) | | |
| 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** |
| 99.40.16.129 |

|  |  |  |
| --- | --- | --- |
| **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:**  MS10-012: Vulnerabilidades en el servidor SMB podrían 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** |
| 99.40.16.139 |

|  |  |  |
| --- | --- | --- |
| **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 KB2719662: Vulnerabilidades en Gadgets podría permitir la ejecución de código remoto  MS08-069: Ejecución remota de código sobre Microsoft XML Core Services (955218)  MS10-012: Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código  MS11-007: Vulnerabilidad en el controlador del OpenType Compact Font Format (CFF) podría permitir la ejecución remota de código  MS11-015: Vulnerabilidades en Windows Media podrían permitir la ejecución remota de código  MS11-019: Vulnerabilidades en SMB Client permiten la ejecución de código remoto.  MS11-020: Vulnerabilidad en SMB server podría resultar en ejecución remota de código (2508429)  MS11-024: Vulnerabilidad en el editor Windows Fax Cover Page permite la ejecución de código remoto.  MS11-027: Actualización de seguridad acumulativa para ActiveX  MS11-030: Vulnerabilidad en la resolución DNS podría permitir la ejecución remota de código  MS11-031: Vulnerabilidad en los motores de scripting de JScript y VBScript podría permitir la ejecución remota de código.  MS11-032: Vulnerabilidad en el controlador OpenType Compact Font Format (CFF) podría permitir la ejecución remota de código.  MS11-038: Vulnerabilidades en OLE Automation podrían permitir ejecución de código remoto (2476490)  MS11-043: Una vulnerabilidad en el cliente SMB podrían permitir la ejecución remota de código (2536276)  MS11-046: Vulnerabilidad en Ancillary Function Driver podría permitir ejecución de código remota (2503665)  MS11-048: Vulnerabilidad en SMB Server podría permitir una denegación de servicio (2536275)  MS11-071 Vulnerabilidad en componentes de windows podría permitir ejecución de código de manera remota.  MS11-075: Vulnerabilidad en Microsoft Active Accessibility podría permitir la ejecución remota de código (2623699)  MS11-076: Vulnerabilidad en Windows Media Center podría permitir la ejecución remota (2604926)  MS11-085: Vulnerabilidad en Windows Mail and Windows Meeting Space podría permitir la ejecución remota de código (2620704)  MS11-090: ActualizaciÃ³n de seguridad para ActiveX  MS11-092: Una vulnerabilidad en Windows Media podría permitir la ejecución remota de código  MS11-097: Una vulnerabilidad en el subsistema de Windows en tiempo de ejecuciÃ³n cliente / servidor podrÃ­a permitir la elevaciÃ³n de privilegios  "MS12-074: Vulnerabilidad en .NET Framework podría permitir la ejecución de código remoto (2745030)  "  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  MS12-081: Vulnerabilidad en Windows en el componente de manejo de archivos podría permitir la ejecución de código remoto (2758857)  MS12-082: Vulnerabiloidad en DirectPlay podría permitir la ejecución de código remoto (2770660)  MS13-001: Vulnerabilidad en Windows Print Spooler Components podría permitir la ejecución remota de código (2769369)  MS13-002: Vulnerabilidad en Microsoft XML podria permitir la ejecución de código remoto (2756145)  MS13-004: Vulnerabilidad en .NET Framework podría permitir la elevación de privilegios (2769324)  MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277)  MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113)  MS13-021: Actualizaciones de seguridad para Internet Explorer (2809289)  MS13-022: Vulnerabilidad en Microsoft Silverlight podría permitir ejecución de código remoto (2814124)  MS13-027: Vulnerabilidad en Kernel-Mode Drivers podría permitir elevación de privilegios de seguridad (2807986) | | |
| 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** |
| 99.40.16.154 |

|  |  |  |
| --- | --- | --- |
| **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:**  MS11-020: SMB presenta fallas en su implementación que permite la ejecución de código remoto | | |
| 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** |
| 99.40.16.173 |

|  |  |  |
| --- | --- | --- |
| **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:**  MS11-048: Vulnerabilidad en SMB Server podría ocasionar una denegación de servicio (2536275) | | |
| 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** |
| 99.40.16.174 |

|  |  |  |
| --- | --- | --- |
| **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:**  MS11-048: Vulnerabilidad en SMB Server podría ocasionar una denegación de servicio (2536275) | | |
| 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** |
| 99.40.16.179 |

|  |  |  |
| --- | --- | --- |
| **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:**  MS10-012: Vulnerabilidades en el servidor SMB podrían 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** |
| 99.40.16.252 |

|  |  |  |
| --- | --- | --- |
| **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:**  MS11-048: Vulnerabilidad en SMB Server podría ocasionar una denegación de servicio (2536275) | | |
| 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** |
| 99.40.16.139 |

|  |  |  |
| --- | --- | --- |
| **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  MS11-009: Vulnerabilidad los motores de scripting de JScript y VBScript podrían permitir la divulgación de información  MS11-026: Vulnerabilidad en MHTML podría permitir la divulgación de información  MS11-037: Múltiples Vulnerabilidades en MHTML podrían permitir revelación de información (2544893)  MS11-066: Una vulnerabilidad en el control Microsoft Chart podría permitir la divulgación de información  MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)  MS13-006: Vulnerabilidad en Microsoft Windows podría permitir la evasión de restricciones de seguridad (2785220)  MS13-007: Vulnerabilidad en Open Data Protocol podría permitir una denegación de servicio (2769327) | | |
| 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. | | |