**Segmento 99.41.24.0**

### 

### Vulnerabilidades de prioridad Media para Administración Local De Recaudación De Tepic

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.24.115 |

|  |  |  |
| --- | --- | --- |
| **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 KB982316: elevación de privilegios a través de evadir Windows Service Isolation  MS13-037: Actualización de Seguridad Acumulativa para Internet Explorer (2829530) | | |
| 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** |
| 99.41.24.123 |

|  |  |  |
| --- | --- | --- |
| **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  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)  MS13-018: Vulnerabilidad en TCP/IP que podría permitir causar una denegación de servicio (2790655)  MS13-037: Actualización de Seguridad Acumulativa para Internet Explorer (2829530)  MS13-038: Actualización de Seguridad Acumulativa para Internet Explorer (2847204)  MS13-040: Vulnerabilidad en .NET Framework podría permitir la suplantación de identidad (2836440) | | |
| 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** |
| 99.41.24.167 |

|  |  |  |
| --- | --- | --- |
| **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  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)  MS13-018: Vulnerabilidad en TCP/IP que podría permitir causar una denegación de servicio (2790655)  MS13-037: Actualización de Seguridad Acumulativa para Internet Explorer (2829530)  MS13-038: Actualización de Seguridad Acumulativa para Internet Explorer (2847204)  MS13-040: Vulnerabilidad en .NET Framework podría permitir la suplantación de identidad (2836440) | | |
| 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** |
| 99.41.24.19 |

|  |  |  |
| --- | --- | --- |
| **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)  MS13-018: Vulnerabilidad en TCP/IP que podría permitir causar una denegación de servicio (2790655)  MS13-037: Actualización de Seguridad Acumulativa para Internet Explorer (2829530)  MS13-038: Actualización de Seguridad Acumulativa para Internet Explorer (2847204)  MS13-040: Vulnerabilidad en .NET Framework podría permitir la suplantación de identidad (2836440) | | |
| 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** |
| 99.41.24.201 |

|  |  |  |
| --- | --- | --- |
| **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 KB2718704: Certificados Digitales podrían permitir suplantación de identidad  MS KB982316: elevación de privilegios a través de evadir Windows Service Isolation  MS08-037: Vulnerabilidad en DNS podría permitir suplantación de identidad (953230)  MS10-037: Vulnerabilidad en el formato OpenType Fuente Compacto (CFF) El controlador podría permitir la elevación de privilegios  MS10-070: Vulnerabilidad en ASP.NET podría permitir la revelación de información (2418042)  MS11-026: Vulnerabilidad en MHTML podría permitir la divulgación de información  MS11-037: Múltiples Vulnerabilidades en MHTML podrían permitir revelación de información (2544893)  MS11-069: Vulnerabilidad en NET Framework podría permitir la divulgación de información (2.567.951)  MS11-074: Vulnerabilidad en Microsoft SharePoint podría permitir elevación de privilegios (2451858)  MS12-003: Vulnerabilidad en el Subsistema de Windows Client/Server Run-time podría permitir elevación de privilegios (2646524)  MS12-006: Vulnerabilidad en SSL/TLS podría permitir revelación de información sensible (2643584)  MS12-049: Vulnerabilidad en TLS Could podría revelar información sensible (2655992)  MS13-037: Actualización de Seguridad Acumulativa para Internet Explorer (2829530)  MS13-040: Vulnerabilidad en .NET Framework podría permitir la suplantación de identidad (2836440) | | |
| 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** |
| 99.41.24.220 |

|  |  |  |
| --- | --- | --- |
| **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 KB982316: elevación de privilegios a través de evadir Windows Service Isolation  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)  MS13-037: Actualización de Seguridad Acumulativa para Internet Explorer (2829530)  MS13-040: Vulnerabilidad en .NET Framework podría permitir la suplantación de identidad (2836440) | | |
| 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** |
| 99.41.24.30 |

|  |  |  |
| --- | --- | --- |
| **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)  MS13-037: Actualización de Seguridad Acumulativa para Internet Explorer (2829530)  MS13-038: Actualización de Seguridad Acumulativa para Internet Explorer (2847204)  MS13-040: Vulnerabilidad en .NET Framework podría permitir la suplantación de identidad (2836440) | | |
| 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. | | |