**Segmento 10.113.2.0**

### 

### Vulnerabilidades de prioridad Alta para Administración Local De Recaudación De Saltillo Norte Centro

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 10.113.2.100 |

|  |  |  |
| --- | --- | --- |
| **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:**  MS05-027: Ejecución de código a través de SMB (896422)  MS06-035: El servicio Server es susceptible a ejecución remota de código (917159)  MS06-040: El servicio Server es susceptible a ejecución remota de código (921883)  MS09-001: Ejecución de código a través de SMB (958687)  MS12-020: Vulnerabilidad en Remote Desktop podría permitir la ejecución de código remoto (2671387) | | |
| 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** |
| 10.113.2.69 |

|  |  |  |
| --- | --- | --- |
| **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:**  MS12-020: Vulnerabilidad en Remote Desktop podría permitir la ejecución de código remoto (2671387) | | |
| 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** |
| 10.113.2.87 |

|  |  |  |
| --- | --- | --- |
| **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:**  MS08-067: Vulnerabilidad en el manejo de peticiones RPC en Microsoft Windows Server Service (958644)  MS09-001: Ejecución de código a través de SMB (958687)  MS12-020: Vulnerabilidad en Remote Desktop podría permitir la ejecución de código remoto (2671387) | | |
| 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** |
| 10.113.2.88 |

|  |  |  |
| --- | --- | --- |
| **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:**  MS08-067: Vulnerabilidad en el manejo de peticiones RPC en Microsoft Windows Server Service (958644)  MS09-001: Ejecución de código a través de SMB (958687)  MS12-020: Vulnerabilidad en Remote Desktop podría permitir la ejecución de código remoto (2671387) | | |
| 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** |
| 10.113.2.90 |

|  |  |  |
| --- | --- | --- |
| **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:**  MS05-027: Ejecución de código a través de SMB (896422)  MS06-035: El servicio Server es susceptible a ejecución remota de código (917159)  MS06-040: El servicio Server es susceptible a ejecución remota de código (921883)  MS08-067: Vulnerabilidad en el manejo de peticiones RPC en Microsoft Windows Server Service (958644)  MS09-001: Ejecución de código a través de SMB (958687)  MS12-020: Vulnerabilidad en Remote Desktop podría permitir la ejecución de código remoto (2671387) | | |
| 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** |
| 10.113.2.91 |

|  |  |  |
| --- | --- | --- |
| **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:**  MS12-020: Vulnerabilidad en Remote Desktop podría permitir la ejecución de código remoto (2671387) | | |
| 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** |
| 10.113.2.92 |

|  |  |  |
| --- | --- | --- |
| **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:**  MS05-027: Ejecución de código a través de SMB (896422)  MS06-035: El servicio Server es susceptible a ejecución remota de código (917159)  MS06-040: El servicio Server es susceptible a ejecución remota de código (921883)  MS09-001: Ejecución de código a través de SMB (958687)  MS12-020: Vulnerabilidad en Remote Desktop podría permitir la ejecución de código remoto (2671387) | | |
| 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** |
| 10.113.2.93 |

|  |  |  |
| --- | --- | --- |
| **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:**  MS05-027: Ejecución de código a través de SMB (896422)  MS06-035: El servicio Server es susceptible a ejecución remota de código (917159)  MS06-040: El servicio Server es susceptible a ejecución remota de código (921883)  MS09-001: Ejecución de código a través de SMB (958687)  MS12-020: Vulnerabilidad en Remote Desktop podría permitir la ejecución de código remoto (2671387) | | |
| 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** |
| 10.113.2.94 |

|  |  |  |
| --- | --- | --- |
| **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:**  MS05-027: Ejecución de código a través de SMB (896422)  MS06-035: El servicio Server es susceptible a ejecución remota de código (917159)  MS06-040: El servicio Server es susceptible a ejecución remota de código (921883)  MS08-067: Vulnerabilidad en el manejo de peticiones RPC en Microsoft Windows Server Service (958644)  MS09-001: Ejecución de código a través de SMB (958687)  MS12-020: Vulnerabilidad en Remote Desktop podría permitir la ejecución de código remoto (2671387) | | |
| 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** |
| 10.113.2.95 |

|  |  |  |
| --- | --- | --- |
| **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:**  MS05-027: Ejecución de código a través de SMB (896422)  MS06-035: El servicio Server es susceptible a ejecución remota de código (917159)  MS06-040: El servicio Server es susceptible a ejecución remota de código (921883)  MS08-067: Vulnerabilidad en el manejo de peticiones RPC en Microsoft Windows Server Service (958644)  MS09-001: Ejecución de código a través de SMB (958687)  MS12-020: Vulnerabilidad en Remote Desktop podría permitir la ejecución de código remoto (2671387) | | |
| 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** |
| 10.113.2.96 |

|  |  |  |
| --- | --- | --- |
| **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:**  MS12-020: Vulnerabilidad en Remote Desktop podría permitir la ejecución de código remoto (2671387) | | |
| 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** |
| 10.113.2.97 |

|  |  |  |
| --- | --- | --- |
| **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:**  MS05-027: Ejecución de código a través de SMB (896422)  MS06-035: El servicio Server es susceptible a ejecución remota de código (917159)  MS06-040: El servicio Server es susceptible a ejecución remota de código (921883)  MS09-001: Ejecución de código a través de SMB (958687)  MS10-012: Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código  MS10-054: Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código  MS11-020: SMB presenta fallas en su implementación que permite la ejecución de código remoto  MS12-020: Vulnerabilidad en Remote Desktop podría permitir la ejecución de código remoto (2671387) | | |
| 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** |
| 10.113.2.98 |

|  |  |  |
| --- | --- | --- |
| **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:**  MS05-027: Ejecución de código a través de SMB (896422)  MS06-035: El servicio Server es susceptible a ejecución remota de código (917159)  MS06-040: El servicio Server es susceptible a ejecución remota de código (921883)  MS08-067: Vulnerabilidad en el manejo de peticiones RPC en Microsoft Windows Server Service (958644)  MS09-001: Ejecución de código a través de SMB (958687)  MS10-012: Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código  MS10-054: Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código  MS11-020: SMB presenta fallas en su implementación que permite la ejecución de código remoto  MS12-020: Vulnerabilidad en Remote Desktop podría permitir la ejecución de código remoto (2671387) | | |
| 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** |
| 10.113.2.99 |

|  |  |  |
| --- | --- | --- |
| **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:**  MS06-035: El servicio Server es susceptible a ejecución remota de código (917159)  MS12-020: Vulnerabilidad en Remote Desktop podría permitir la ejecución de código remoto (2671387) | | |
| 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** |
| 10.113.2.97 |

|  |  |  |
| --- | --- | --- |
| **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:**  MS06-008: Vulnerabilidad en Web Client Service provoca ejecución remota de código (911927) | | |
| 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** |
| 10.113.2.98 |

|  |  |  |
| --- | --- | --- |
| **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:**  MS06-008: Vulnerabilidad en Web Client Service provoca ejecución remota de código (911927) | | |
| 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. | | |

**\*\*\*\*\*\*  
ALTA  
  
\*\*\*\*\*\***  
MS05-027: Ejecución de código a través de SMB (896422)

MS06-035: El servicio Server es susceptible a ejecución remota de código (917159)

MS06-040: El servicio Server es susceptible a ejecución remota de código (921883)

MS08-067: Vulnerabilidad en el manejo de peticiones RPC en Microsoft Windows Server Service (958644)

MS09-001: Ejecución de código a través de SMB (958687)

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

MS10-054: Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código

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

MS12-020: Vulnerabilidad en Remote Desktop podría permitir la ejecución de código remoto (2671387)

**\*\*\*\*\*\*  
MEDIA  
  
\*\*\*\*\*\*\*\***MS06-008: Vulnerabilidad en Web Client Service provoca ejecución remota de código (911927)