**Segmento 99.53.24.0**

### 

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

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.53.24.120 |

|  |  |  |
| --- | --- | --- |
| **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 KB2488013: Internet Explorer no procesa correctamente CSS  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  MS09-053: Vulnerabilidades en el servicio FTP de Internet Information Services (IIS) podría permitir la ejecución de código remoto  MS09-062: Vulnerabilidades en GDI+ podrían permitir la ejecución remota de código  MS11-002: Vulnerabilidades en Microsoft Data Access Components que podrían permitir la ejecución remota de código  MS11-003: IE Actualización de seguridad acumulativa para Internet Explorer  MS11-006: Una vulnerabilidad en el procesamiento de gráficos de la Shell de Windows podría permitir la ejecución remota de código (2483185)  MS11-007: Vulnerabilidad en el controlador del OpenType Compact Font Format (CFF) podría permitir la ejecución remota de código  MS11-011: Vulnerabilidades en el kernel de Windows podrían permitir la elevación de privilegios  MS11-012: Vulnerabilidades en el Kernel deWindows podría permitir la elevación de privilegios  MS11-013: Vulnerabilidades en Kerberos podrían permitir la elevación de privilegios  MS11-014: Vulnerabilidad en Local Security Authority Subsystem Service podría permitir elevación de privilegios localmente (2478960)  MS11-018: Actualización de seguridad acumulativa para Internet Explorer (2497640)  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  MS11-028: Vulnerabilidad en .NET Framework, podría permitir la ejecución de código arbitrario  MS11-029: Vulnerability in GDI+ podría permitir la ejecución remota de código  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.  MS11-033: Vulnerabilidad en WordPad Text Converters podría permitir la ejecución de código remoto (2485663)  MS11-034: Vulnerabilidades en los controladores Windows Kernel-Mode, podrían permitir la elevación de privilegios.  MS11-038: Vulnerabilidades en OLE Automation podrían permitir ejecución de código remoto (2476490)  MS11-039: Vulnerabilidad en .NET y Microsoft Silverlight podría permitir ejecución remota de código (2514842)  MS11-042: Vulnerabilidades en Distributed File System podrían permitir ejecución de código remoto (2535512)  MS11-043: Una vulnerabilidad en el cliente SMB podrían permitir la ejecución remota de código (2536276)  MS11-044: Vulnerabilidad en .NET Framework podría permitir ejecución de código remota (2538814)  MS11-046: Vulnerabilidad en Ancillary Function Driver podría permitir ejecución de código remota (2503665)  MS11-050: Actualización de seguridad acumulativa para Internet Explorer (2530548)  MS11-052: Vulnerabilidad en Vector Markup Language podría permitir ejecución remota de código (2544521)  MS11-054: Vulnerabilidad en Windows Kernel-Mode Drivers podría permitir una elevación de privilegios (2555917)  MS11-057: Actualización de seguridad acumulativa para Internet Explorer (2559049)  MS11-062: Vulnerabilidad en el controlador de Remote Access Service NDISTAPI podría permitir la elevación de privilegios (2566454)  MS11-063 Vulnerabilidad en el subsistema cliente/servidor en tiempo de ejecución podría permitir la elevación de privilegios.  MS11-065: Vulnerabilidad en Remote Desktop Protocol podría permitir una denegación de servicio (2570222)  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)  MS11-077: Vulnerabilidades en los controladores de Windows Kernel-Mode podrían permitir ejecución remota de código (2567053)  MS11-078: Vulnerabilidad en .NET Framework y Microsoft Silverlight podría permitir ejecución remota de código (2604930)  MS11-080: Vulnerabilidad en driver de función auxiliar podría permitir la elevación de privilegios  MS11-081: Actualización de seguridad acumulativa para Internet Explorer (2586448)  MS11-087: Vulnerabilidad en Microsoft en el kernel de Windows podrÃ­an permitir la ejecuciÃ³n remota de cÃ³digo  MS11-090: ActualizaciÃ³n de seguridad para ActiveX  MS11-093: Vulnerabilidad en OLE podría permitir ejecución de código remoto(2624667)  MS11-097: Una vulnerabilidad en el subsistema de Windows en tiempo de ejecuciÃ³n cliente / servidor podrÃ­a permitir la elevaciÃ³n de privilegios  MS11-098: Vulnerabilidad en Microsoft en el kernel de Windows podrían permitir la elevación de privilegios  MS11-099: Actualización de seguridad para Internet Explorer  MS11-100: Vulnerabilidad en .NET Framework podría permitir elevación de privilegios (2638420)  MS12-001: Vulnerabilidad en Windows Kernel podría permitir evasión de politicas de seguridad (2644615)  MS12-002: Vulnerabilidad en Windows Object Packager podría permitir ejecucón remota de código (2603381)  MS12-004: Vulnerabilidad en Windows Media podría permitir ejecución de código remoto (2636391)  MS12-005: Vulnerabilidad en Microsoft Windows podría permitir ejecución de código remoto (2584146)  MS12-008: Vulnerabilidades en el Kernel-Mode Drivers de Microsoft Windows podría permitir la ejecución de código remoto (2660465)  MS12-009: Vulnerabilidad en Ancillary Function Driver podría permitir la elevación de privilegios (2645640)  MS12-010: Actualizaciones de parches de seguridad acumulativos para Internet Explorer (2647516)  MS12-016: Vulnerabilidad en .NET Framework y Microsoft Silverlight podrían permitir ejecución de código remoto (2651026)  MS12-020: Vulnerabilidad en Remote Desktop podría permitir la ejecución de código remoto (2671387)  MS12-020: Vulnerabilidades en Escritorio remoto podrían permitir la ejecución de código (2671387)  MS12-023: Actualización Acumulativa de Seguridad para Internet Explorer (2675157)  MS12-024: Vulnerabilidad en Windows podría permitir la ejecución remota de código (2653956)  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)  MS12-034: Actualizaciones de Seguridad para Microsoft Office, Windows, .NET Framework, y Silverlight (2681578)  MS12-035: Vulnerabilidad en .NET Framework podría permitir ejecución remota de código (2693777)  MS12-036: Vulnerabilidad en Remote Desktop podría permitir la ejecución de código remoto (2685939)  MS12-037: Actualización acumulativa de seguridad para Internet Explorer (2699988)  MS12-038: Vulnerabilidad en .NET Framework podría permitir ejecución ed código remoto (2706726)  MS12-041: Vulnerabilidades en los drivers del Kernel-Mode de Windows podrían permitir la elevación de privilegios (2709162)  MS12-042: Vulnerabilidades en el Kernel de Windows podrían permitir la elevación de privileagios (2711167)  MS12-043: Vulnerabilidades en Microsoft XML Core Services podrían permitir la ejecución de código remoto (2722479)  MS12-045: Vulnerabilidad en Microsoft Data Access Components podría permitir la ejecución de código remoto (2698365)  MS12-047: Vulnerabilidades en los drivers de Kernel-Mode de Windows podrían permitir la elevación de privilegios (2718523)  MS12-048: Vulnerabilidad en Windows Shell podría permitir la ejecución de código remoto (2691442)  MS12-052: Actualizaciones de seguridad acumulativas para Internet Explorer (2722913)  MS12-054: Múltiples vulnerabilidades en Windows Networking Components(2733594)  MS12-055: Vulnerabilidad en Windows Kernel-Mode Drivers permite la elevación de privilegios (2731847)  MS12-060: Vulnerabilidad en Windows Common Controls podría permitir la ejecución de código remoto (2720573)  MS12-063: Actualización acumulativa de seguridad para Internet Explorer (2744842)  MS12-068: Vulnerabilidad en el Windows Kernel podría permitir la elevación de privilegios (2724197)  MS12-072: Vulnerabilidad en Windows Shell podría permitir la ejecución de código remoto (2727528)  "MS12-074: Vulnerabilidad en .NET Framework podría permitir la ejecución de código remoto (2745030)  "  MS12-075: Vulnerabilidad en drivers del kernel de Windows podrían permitir la ejecución de código remoto(2761226)  MS12-077: Actualización de Seguridad para Internet Explorer (2761465)  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)  MS13-002: 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)  MS13-008: Actualización de seguridad acumulativa para Internet Explorer (2799329)  MS13-009: Actualización de seguridad para Internet Explorer (2792100)  MS13-010: Vulnerabilidad en Vector Markup Language (VML) que podría permitir la ejecución remota de código (2797052)  MS13-011: Vulnerabilidad en Media Decompression que podría permitir la ejecución remota de código (2780091)  MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277)  MS13-016: Vulnerabilidades en Windows Kernel-Mode Driver que podrían permitir la elevación de privilegios (2778344)  MS13-017: Vulnerabilidades en Windows Kernel que podrían permitir la elevación de privilegios (2799494) | | |
| 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** |
| 99.53.24.122 |

|  |  |  |
| --- | --- | --- |
| **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  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)  MS10-059: 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)  MS13-008: Actualización de seguridad acumulativa para Internet Explorer (2799329)  MS13-009: Actualización de seguridad para Internet Explorer (2792100)  MS13-010: Vulnerabilidad en Vector Markup Language (VML) que podría permitir la ejecución remota de código (2797052)  MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277)  MS13-016: Vulnerabilidades en Windows Kernel-Mode Driver que podrían permitir la elevación de privilegios (2778344)  MS13-017: Vulnerabilidades en Windows Kernel que podrían permitir la elevación de privilegios (2799494)  MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113) | | |
| 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** |
| 99.53.24.125 |

|  |  |  |
| --- | --- | --- |
| **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  MS08-018: Microsoft Project permite ejecución de código (950183)  MS08-069: Ejecución remota de código sobre Microsoft XML Core Services (955218)  MS09-035: Múltiples Vulnerabilidades en Visual Studio Active Template Library permiten de manera remota la ejecución de código (969706)  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)  MS10-059: 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)  MS11-050: Actualización de seguridad acumulativa para Internet Explorer (2530548)  MS11-057: Actualización de seguridad acumulativa para Internet Explorer (2559049)  MS11-081: Actualización de seguridad acumulativa para Internet Explorer (2586448)  MS11-099: Actualización de seguridad para Internet Explorer  MS12-010: Actualizaciones de parches de seguridad acumulativos para Internet Explorer (2647516)  MS12-023: Actualización Acumulativa de Seguridad para Internet Explorer (2675157)  MS12-037: Actualización acumulativa de seguridad para Internet Explorer (2699988)  MS12-044: Actualización de seguridad Acumulativa para Internet Explorer (2719177)  MS12-052: Actualizaciones de seguridad acumulativas para Internet Explorer (2722913)  MS12-063: Actualización acumulativa de seguridad para Internet Explorer (2744842)  MS12-071: Actualización de Seguridad para Internet Explorer (2761451)  MS12-077: Actualización de Seguridad para Internet Explorer (2761465)  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  MS13-009: Actualización de seguridad para Internet Explorer (2792100)  MS13-010: Vulnerabilidad en Vector Markup Language (VML) que podría permitir la ejecución remota de código (2797052)  MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277)  MS13-016: Vulnerabilidades en Windows Kernel-Mode Driver que podrían permitir la elevación de privilegios (2778344)  MS13-017: Vulnerabilidades en Windows Kernel que podrían permitir la elevación de privilegios (2799494)  MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113) | | |
| 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** |
| 99.53.24.127 |

|  |  |  |
| --- | --- | --- |
| **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 ejecucion remota de codigo  MS08-015: Vulnerabilidad en Microsoft Outlook  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  MS09-009: Vulnerabilidades en Microsoft Office Excel podrían permitir ejecucion remota de codigo  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 ejecucion remota de codigo  MS09-030: Vulnerabilidad en Microsoft Office Publisher podría permitir la ejecución de código remoto (969516)  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)  MS10-012: Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código  MS10-017: Vulnerabilidades en Microsoft Office Excel podrían permitir la ejecución remota de código (980150)  MS10-023: Vulnerabilidad en Microsoft Office Publisher podría permitir la ejecucion remota de codigo  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)  MS10-045: Vulnerabilidad en Microsoft Outlook  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)  MS10-080: Vulnerabilidades en Microsoft Excel podrían permitir la ejecución remota de código (2293211)  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)  MS10-103: 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)  MS11-072: Vulnerabilidades en Microsoft Excel podría permitir la ejecución remota de código (2587505)  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)  "MS12-074: 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)  MS13-002: Vulnerabilidad en Microsoft XML podria permitir la ejecución de código remoto (2756145)  MS13-008: Actualización de seguridad acumulativa para Internet Explorer (2799329)  MS13-009: Actualización de seguridad para Internet Explorer (2792100)  MS13-010: Vulnerabilidad en Vector Markup Language (VML) que podría permitir la ejecución remota de código (2797052)  MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277)  MS13-016: Vulnerabilidades en Windows Kernel-Mode Driver que podrían permitir la elevación de privilegios (2778344)  MS13-017: Vulnerabilidades en Windows Kernel que podrían permitir la elevación de privilegios (2799494)  MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113) | | |
| 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** |
| 99.53.24.128 |

|  |  |  |
| --- | --- | --- |
| **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  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)  MS10-059: 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)  MS13-008: Actualización de seguridad acumulativa para Internet Explorer (2799329)  MS13-009: Actualización de seguridad para Internet Explorer (2792100)  MS13-010: Vulnerabilidad en Vector Markup Language (VML) que podría permitir la ejecución remota de código (2797052)  MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277)  MS13-016: Vulnerabilidades en Windows Kernel-Mode Driver que podrían permitir la elevación de privilegios (2778344)  MS13-017: Vulnerabilidades en Windows Kernel que podrían permitir la elevación de privilegios (2799494)  MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113) | | |
| 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** |
| 99.53.24.130 |

|  |  |  |
| --- | --- | --- |
| **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)  MS10-059: 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)  MS13-008: Actualización de seguridad acumulativa para Internet Explorer (2799329)  MS13-009: Actualización de seguridad para Internet Explorer (2792100)  MS13-010: Vulnerabilidad en Vector Markup Language (VML) que podría permitir la ejecución remota de código (2797052)  MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277)  MS13-016: Vulnerabilidades en Windows Kernel-Mode Driver que podrían permitir la elevación de privilegios (2778344)  MS13-017: Vulnerabilidades en Windows Kernel que podrían permitir la elevación de privilegios (2799494)  MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113) | | |
| 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** |
| 99.53.24.137 |

|  |  |  |
| --- | --- | --- |
| **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  MS08-069: Ejecución remota de código sobre Microsoft XML Core Services (955218)  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)  MS10-059: 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  "MS12-074: 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)  MS13-004: Vulnerabilidad en .NET Framework podría permitir la elevación de privilegios (2769324)  MS13-008: Actualización de seguridad acumulativa para Internet Explorer (2799329)  MS13-009: Actualización de seguridad para Internet Explorer (2792100)  MS13-010: Vulnerabilidad en Vector Markup Language (VML) que podría permitir la ejecución remota de código (2797052)  MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277)  MS13-016: Vulnerabilidades en Windows Kernel-Mode Driver que podrían permitir la elevación de privilegios (2778344)  MS13-017: Vulnerabilidades en Windows Kernel que podrían permitir la elevación de privilegios (2799494)  MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113) | | |
| 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** |
| 99.53.24.141 |

|  |  |  |
| --- | --- | --- |
| **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)  MS10-019: Vulnerabilidades en Windows podrían permitir la ejecución de código (981210)  MS10-033: Vulnerabilidades en la descompresión de archivos multimedia, podrían permitir la ejecución remota de código(979902)  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)  MS11-004: Internet Information Services (IIS) en el servicio FTP podría permitir la ejecución de código remoto  MS11-091: Vulnerabilidad en Microsoft Publisher podría permitir la ejecución remota de código  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  MS13-008: Actualización de seguridad acumulativa para Internet Explorer (2799329)  MS13-009: Actualización de seguridad para Internet Explorer (2792100)  MS13-010: Vulnerabilidad en Vector Markup Language (VML) que podría permitir la ejecución remota de código (2797052)  MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277)  MS13-016: Vulnerabilidades en Windows Kernel-Mode Driver que podrían permitir la elevación de privilegios (2778344)  MS13-017: Vulnerabilidades en Windows Kernel que podrían permitir la elevación de privilegios (2799494)  MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113) | | |
| 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** |
| 99.53.24.144 |

|  |  |  |
| --- | --- | --- |
| **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)  MS10-059: 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)  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)  MS13-008: Actualización de seguridad acumulativa para Internet Explorer (2799329)  MS13-009: Actualización de seguridad para Internet Explorer (2792100)  MS13-010: Vulnerabilidad en Vector Markup Language (VML) que podría permitir la ejecución remota de código (2797052)  MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277)  MS13-016: Vulnerabilidades en Windows Kernel-Mode Driver que podrían permitir la elevación de privilegios (2778344)  MS13-017: Vulnerabilidades en Windows Kernel que podrían permitir la elevación de privilegios (2799494)  MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113) | | |
| 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** |
| 99.53.24.169 |

|  |  |  |
| --- | --- | --- |
| **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** |
| 99.53.24.171 |

|  |  |  |
| --- | --- | --- |
| **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:**  MS08-067: Vulnerabilidad en el manejo de peticiones RPC en Microsoft Windows Server Service (958644)  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** |
| 99.53.24.187 |

|  |  |  |
| --- | --- | --- |
| **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  MS08-070: Vulnerabilidades en controles de Visual Basic 6.0 ActiveX pueden 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)  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)  MS10-059: 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)  MS13-008: Actualización de seguridad acumulativa para Internet Explorer (2799329)  MS13-009: Actualización de seguridad para Internet Explorer (2792100)  MS13-010: Vulnerabilidad en Vector Markup Language (VML) que podría permitir la ejecución remota de código (2797052)  MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277)  MS13-016: Vulnerabilidades en Windows Kernel-Mode Driver que podrían permitir la elevación de privilegios (2778344)  MS13-017: Vulnerabilidades en Windows Kernel que podrían permitir la elevación de privilegios (2799494)  MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113) | | |
| 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** |
| 99.53.24.211 |

|  |  |  |
| --- | --- | --- |
| **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)  MS10-059: 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)  MS13-008: Actualización de seguridad acumulativa para Internet Explorer (2799329)  MS13-009: Actualización de seguridad para Internet Explorer (2792100)  MS13-010: Vulnerabilidad en Vector Markup Language (VML) que podría permitir la ejecución remota de código (2797052)  MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277)  MS13-016: Vulnerabilidades en Windows Kernel-Mode Driver que podrían permitir la elevación de privilegios (2778344)  MS13-017: Vulnerabilidades en Windows Kernel que podrían permitir la elevación de privilegios (2799494)  MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113) | | |
| 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** |
| 99.53.24.224 |

|  |  |  |
| --- | --- | --- |
| **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)  MS10-059: 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)  MS13-008: Actualización de seguridad acumulativa para Internet Explorer (2799329)  MS13-009: Actualización de seguridad para Internet Explorer (2792100)  MS13-010: Vulnerabilidad en Vector Markup Language (VML) que podría permitir la ejecución remota de código (2797052)  MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277)  MS13-016: Vulnerabilidades en Windows Kernel-Mode Driver que podrían permitir la elevación de privilegios (2778344)  MS13-017: Vulnerabilidades en Windows Kernel que podrían permitir la elevación de privilegios (2799494)  MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113) | | |
| 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** |
| 99.53.24.240 |

|  |  |  |
| --- | --- | --- |
| **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)  MS10-059: 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  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  MS13-008: Actualización de seguridad acumulativa para Internet Explorer (2799329)  MS13-009: Actualización de seguridad para Internet Explorer (2792100)  MS13-010: Vulnerabilidad en Vector Markup Language (VML) que podría permitir la ejecución remota de código (2797052)  MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277)  MS13-016: Vulnerabilidades en Windows Kernel-Mode Driver que podrían permitir la elevación de privilegios (2778344)  MS13-017: Vulnerabilidades en Windows Kernel que podrían permitir la elevación de privilegios (2799494)  MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113) | | |
| 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** |
| 99.53.24.43 |

|  |  |  |
| --- | --- | --- |
| **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  MS08-019: Microsoft Visio permite la ejecución de código remoto  MS08-069: Ejecución remota de código sobre Microsoft XML Core Services (955218)  MS08-070: Vulnerabilidades en controles de Visual Basic 6.0 ActiveX pueden permitir la ejecución remota de código  MS09-005: Microsoft Office Visio presenta vulnerabilidad que permite 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)  MS10-036: Vulnerabilidad en la validación de COM en Microsoft Office podría permitir la ejecución remota de código (983235)  MS10-040: Microsoft Internet Information Services (IIS) podría permitir ejecución remota de código  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)  MS11-004: Internet Information Services (IIS) en el servicio FTP podría permitir la ejecución de código remoto  MS11-025: Vulnerabilidad en la librería Microsoft Foundation Class (MFC), podría permitir la ejecución remota de código (2500212)  MS11-050: Actualización de seguridad acumulativa para Internet Explorer (2530548)  MS11-057: Actualización de seguridad acumulativa para Internet Explorer (2559049)  MS11-060: Vulnerabilidades en Microsoft Visio podrían permitir la ejecución remota de código (2560978)  MS11-081: Actualización de seguridad acumulativa para Internet Explorer (2586448)  MS11-091: Vulnerabilidad en Microsoft Publisher podría permitir la ejecución remota de código  MS11-099: Actualización de seguridad para Internet Explorer  MS12-010: Actualizaciones de parches de seguridad acumulativos para Internet Explorer (2647516)  MS12-023: Actualización Acumulativa de Seguridad para Internet Explorer (2675157)  MS12-034: Actualizaciones de Seguridad para Microsoft Office, Windows, .NET Framework, y Silverlight (2681578)  MS12-037: Actualización acumulativa de seguridad para Internet Explorer (2699988)  MS12-039: Vulnerabilidad en Lync podría permitir la ejecución de código remoto (2707956)  MS12-044: Actualización de seguridad Acumulativa para Internet Explorer (2719177)  MS12-052: Actualizaciones de seguridad acumulativas para Internet Explorer (2722913)  MS12-063: Actualización acumulativa de seguridad para Internet Explorer (2744842)  MS12-071: Actualización de Seguridad para Internet Explorer (2761451)  MS12-077: Actualización de Seguridad para Internet Explorer (2761465)  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  MS13-009: Actualización de seguridad para Internet Explorer (2792100)  MS13-010: Vulnerabilidad en Vector Markup Language (VML) que podría permitir la ejecución remota de código (2797052)  MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277)  MS13-016: Vulnerabilidades en Windows Kernel-Mode Driver que podrían permitir la elevación de privilegios (2778344)  MS13-017: Vulnerabilidades en Windows Kernel que podrían permitir la elevación de privilegios (2799494)  MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113) | | |
| 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** |
| 99.53.24.48 |

|  |  |  |
| --- | --- | --- |
| **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  MS10-012: 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)  MS10-059: 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)  MS13-008: Actualización de seguridad acumulativa para Internet Explorer (2799329)  MS13-009: Actualización de seguridad para Internet Explorer (2792100)  MS13-010: Vulnerabilidad en Vector Markup Language (VML) que podría permitir la ejecución remota de código (2797052)  MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277)  MS13-016: Vulnerabilidades en Windows Kernel-Mode Driver que podrían permitir la elevación de privilegios (2778344)  MS13-017: Vulnerabilidades en Windows Kernel que podrían permitir la elevación de privilegios (2799494)  MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113) | | |
| 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** |
| 99.53.24.54 |

|  |  |  |
| --- | --- | --- |
| **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)  MS10-059: 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)  MS13-008: Actualización de seguridad acumulativa para Internet Explorer (2799329)  MS13-009: Actualización de seguridad para Internet Explorer (2792100)  MS13-010: Vulnerabilidad en Vector Markup Language (VML) que podría permitir la ejecución remota de código (2797052)  MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277)  MS13-016: Vulnerabilidades en Windows Kernel-Mode Driver que podrían permitir la elevación de privilegios (2778344)  MS13-017: Vulnerabilidades en Windows Kernel que podrían permitir la elevación de privilegios (2799494)  MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113) | | |
| 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** |
| 99.53.24.57 |

|  |  |  |
| --- | --- | --- |
| **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)  MS10-059: 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)  MS13-008: Actualización de seguridad acumulativa para Internet Explorer (2799329)  MS13-009: Actualización de seguridad para Internet Explorer (2792100)  MS13-010: Vulnerabilidad en Vector Markup Language (VML) que podría permitir la ejecución remota de código (2797052)  MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277)  MS13-016: Vulnerabilidades en Windows Kernel-Mode Driver que podrían permitir la elevación de privilegios (2778344)  MS13-017: Vulnerabilidades en Windows Kernel que podrían permitir la elevación de privilegios (2799494)  MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113) | | |
| 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** |
| 99.53.24.64 |

|  |  |  |
| --- | --- | --- |
| **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  MS10-012: 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)  MS10-059: 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)  MS13-008: Actualización de seguridad acumulativa para Internet Explorer (2799329)  MS13-009: Actualización de seguridad para Internet Explorer (2792100)  MS13-010: Vulnerabilidad en Vector Markup Language (VML) que podría permitir la ejecución remota de código (2797052)  MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277)  MS13-016: Vulnerabilidades en Windows Kernel-Mode Driver que podrían permitir la elevación de privilegios (2778344)  MS13-017: Vulnerabilidades en Windows Kernel que podrían permitir la elevación de privilegios (2799494)  MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113) | | |
| 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** |
| 99.53.24.69 |

|  |  |  |
| --- | --- | --- |
| **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:**  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** |
| 99.53.24.73 |

|  |  |  |
| --- | --- | --- |
| **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  MS08-069: Ejecución remota de código sobre Microsoft XML Core Services (955218)  MS08-070: Vulnerabilidades en controles de Visual Basic 6.0 ActiveX pueden permitir la ejecución remota de código  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)  MS10-059: 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)  MS13-008: Actualización de seguridad acumulativa para Internet Explorer (2799329)  MS13-009: Actualización de seguridad para Internet Explorer (2792100)  MS13-010: Vulnerabilidad en Vector Markup Language (VML) que podría permitir la ejecución remota de código (2797052)  MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277)  MS13-016: Vulnerabilidades en Windows Kernel-Mode Driver que podrían permitir la elevación de privilegios (2778344)  MS13-017: Vulnerabilidades en Windows Kernel que podrían permitir la elevación de privilegios (2799494)  MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113) | | |
| 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** |
| 99.53.24.75 |

|  |  |  |
| --- | --- | --- |
| **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)  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)  MS10-059: 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)  MS13-008: Actualización de seguridad acumulativa para Internet Explorer (2799329)  MS13-009: Actualización de seguridad para Internet Explorer (2792100)  MS13-010: Vulnerabilidad en Vector Markup Language (VML) que podría permitir la ejecución remota de código (2797052)  MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277)  MS13-016: Vulnerabilidades en Windows Kernel-Mode Driver que podrían permitir la elevación de privilegios (2778344)  MS13-017: Vulnerabilidades en Windows Kernel que podrían permitir la elevación de privilegios (2799494)  MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113) | | |
| 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** |
| 99.53.24.79 |

|  |  |  |
| --- | --- | --- |
| **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  MS10-012: 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)  MS10-040: Microsoft Internet Information Services (IIS) podría permitir ejecución remota de código  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)  MS11-004: Internet Information Services (IIS) en el servicio FTP podría permitir la ejecución de código remoto  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 podria 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 privilregios (2778930)  MS13-008: Actualización de seguridad acumulativa para Internet Explorer (2799329)  MS13-009: Actualización de seguridad para Internet Explorer (2792100)  MS13-010: Vulnerabilidad en Vector Markup Language (VML) que podría permitir la ejecución remota de código (2797052)  MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277)  MS13-016: Vulnerabilidades en Windows Kernel-Mode Driver que podrían permitir la elevación de privilegios (2778344)  MS13-017: Vulnerabilidades en Windows Kernel que podrían permitir la elevación de privilegios (2799494)  MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113) | | |
| 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** |
| 99.53.24.85 |

|  |  |  |
| --- | --- | --- |
| **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)  MS10-059: 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)  MS13-008: Actualización de seguridad acumulativa para Internet Explorer (2799329)  MS13-009: Actualización de seguridad para Internet Explorer (2792100)  MS13-010: Vulnerabilidad en Vector Markup Language (VML) que podría permitir la ejecución remota de código (2797052)  MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277)  MS13-016: Vulnerabilidades en Windows Kernel-Mode Driver que podrían permitir la elevación de privilegios (2778344)  MS13-017: Vulnerabilidades en Windows Kernel que podrían permitir la elevación de privilegios (2799494)  MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113) | | |
| 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** |
| 99.53.24.120 |

|  |  |  |
| --- | --- | --- |
| **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 KB2524375: Certificados digitales fraudulentos permiten la suplantación de identidad**  **MS KB2641690: Certificados Digitales Fraudulentos podrÃ­an permitir Spoofing**  **MS KB2718704: Certificados Digitales podrían permitir suplantación de identidad**  **MS KB2728973: Certificados digitales no autorizados podrían permitir la suplantación de identidad**  **MS KB982316: Elevación de privilegios a través de evadir Windows Service Isolation**  **MS11-010: Vulnerabilidad en Windows Client/Server Run-time Subsystem podría permitir la elevación de privilegios (2476687)**  **MS11-026: Vulnerabilidad en MHTML podría permitir la divulgación de información**  **MS11-037: Múltiples Vulnerabilidades en MHTML podrían permitir revelación de información (2544893)**  **MS11-049: Una vulnerabilidad en el Editor XML de Microsoft podría permitir la divulgación de información (2.543.893)**  **MS11-056 Vulnerabilidad en el subsistema cliente/servidor en tiempo de ejecución podría permitir la elevación de privilegios.**  **MS11-069: Vulnerabilidad en NET Framework podría permitir la divulgación de información (2.567.951)**  **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)**  **MS12-018: Vulnerabilidad en los controladores del modo kernel de Windows podría permitir la elevación de privilegios (2641653)**  **MS12-049: Vulnerabilidad en TLS Could podría revelar informaciín sensible (2655992)** | | |
| 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** |
| 99.53.24.122 |

|  |  |  |
| --- | --- | --- |
| **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 KB982316: Elevación de privilegios a través de evadir Windows Service Isolation  MS09-056: Vulnerabilidades en Windows CryptoAPI podrían permitir suplantación de identidad (spoofing)  MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)  MS13-018: Vulnerabilidad en TCP/IP que odría permitir causar una denegación de servicio (2790655) | | |
| 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** |
| 99.53.24.125 |

|  |  |  |
| --- | --- | --- |
| **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)  MS13-018: Vulnerabilidad en TCP/IP que odría permitir causar una denegación de servicio (2790655) | | |
| 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** |
| 99.53.24.127 |

|  |  |  |
| --- | --- | --- |
| **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 KB2718704: Certificados Digitales podrían permitir 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)  MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)  MS13-018: Vulnerabilidad en TCP/IP que odría permitir causar una denegación de servicio (2790655) | | |
| 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** |
| 99.53.24.128 |

|  |  |  |
| --- | --- | --- |
| **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**  **MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)**  **MS13-018: Vulnerabilidad en TCP/IP que odría permitir causar una denegación de servicio (2790655)** | | |
| 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** |
| 99.53.24.130 |

|  |  |  |
| --- | --- | --- |
| **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  MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)  MS13-018: Vulnerabilidad en TCP/IP que odría permitir causar una denegación de servicio (2790655) | | |
| 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** |
| 99.53.24.137 |

|  |  |  |
| --- | --- | --- |
| **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  MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)  MS13-018: Vulnerabilidad en TCP/IP que odría permitir causar una denegación de servicio (2790655) | | |
| 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** |
| 99.53.24.141 |

|  |  |  |
| --- | --- | --- |
| **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)**  **MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)**  **MS12-073: Vulnerabilidad en Microsoft Internet Information Services (IIS) podría permitir la revelación de información (2733829)**  **MS13-018: Vulnerabilidad en TCP/IP que odría permitir causar una denegación de servicio (2790655)** | | |
| 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** |
| 99.53.24.144 |

|  |  |  |
| --- | --- | --- |
| **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)**  **MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)**  **MS13-018: Vulnerabilidad en TCP/IP que odría permitir causar una denegación de servicio (2790655)** | | |
| 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** |
| 99.53.24.187 |

|  |  |  |
| --- | --- | --- |
| **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 KB982316: Elevación de privilegios a través de evadir Windows Service Isolation**  **MS09-056: Vulnerabilidades en Windows CryptoAPI podrían permitir suplantación de identidad (spoofing)**  **MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)**  **MS13-018: Vulnerabilidad en TCP/IP que odría permitir causar una denegación de servicio (2790655)** | | |
| 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** |
| 99.53.24.211 |

|  |  |  |
| --- | --- | --- |
| **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  MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)  MS13-018: Vulnerabilidad en TCP/IP que odría permitir causar una denegación de servicio (2790655) | | |
| 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** |
| 99.53.24.224 |

|  |  |  |
| --- | --- | --- |
| **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)**  **MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)**  **MS13-018: Vulnerabilidad en TCP/IP que odría permitir causar una denegación de servicio (2790655)** | | |
| 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** |
| 99.53.24.240 |

|  |  |  |
| --- | --- | --- |
| **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**  **MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)**  **MS13-018: Vulnerabilidad en TCP/IP que odría permitir causar una denegación de servicio (2790655)** | | |
| 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** |
| 99.53.24.43 |

|  |  |  |
| --- | --- | --- |
| **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 KB982316: Elevación de privilegios a través de evadir Windows Service Isolation  MS10-065: Microsoft Internet Information Services (IIS) permite la ejecución de código remoto  MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)  MS12-073: Vulnerabilidad en Microsoft Internet Information Services (IIS) podría permitir la revelación de información (2733829)  MS13-018: Vulnerabilidad en TCP/IP que odría permitir causar una denegación de servicio (2790655) | | |
| 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** |
| 99.53.24.48 |

|  |  |  |
| --- | --- | --- |
| **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**  **MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)**  **MS13-018: Vulnerabilidad en TCP/IP que odría permitir causar una denegación de servicio (2790655)** | | |
| 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** |
| 99.53.24.54 |

|  |  |  |
| --- | --- | --- |
| **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  MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)  MS13-018: Vulnerabilidad en TCP/IP que odría permitir causar una denegación de servicio (2790655) | | |
| 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** |
| 99.53.24.57 |

|  |  |  |
| --- | --- | --- |
| **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**  **MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)**  **MS13-018: Vulnerabilidad en TCP/IP que odría permitir causar una denegación de servicio (2790655)** | | |
| 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** |
| 99.53.24.64 |

|  |  |  |
| --- | --- | --- |
| **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**  **MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)**  **MS13-018: Vulnerabilidad en TCP/IP que odría permitir causar una denegación de servicio (2790655)** | | |
| 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** |
| 99.53.24.73 |

|  |  |  |
| --- | --- | --- |
| **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 KB982316: Elevación de privilegios a través de evadir Windows Service Isolation  MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)  MS13-018: Vulnerabilidad en TCP/IP que odría permitir causar una denegación de servicio (2790655) | | |
| 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** |
| 99.53.24.75 |

|  |  |  |
| --- | --- | --- |
| **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  MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)  MS13-018: Vulnerabilidad en TCP/IP que odría permitir causar una denegación de servicio (2790655) | | |
| 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** |
| 99.53.24.79 |

|  |  |  |
| --- | --- | --- |
| **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)  MS10-065: Microsoft Internet Information Services (IIS) permite la ejecución de código remoto  MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)  MS12-073: Vulnerabilidad en Microsoft Internet Information Services (IIS) podría permitir la revelación de información (2733829)  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 odría permitir causar una denegación de servicio (2790655) | | |
| 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** |
| 99.53.24.85 |

|  |  |  |
| --- | --- | --- |
| **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 KB982316: Elevación de privilegios a través de evadir Windows Service Isolation**  **MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)**  **MS13-018: Vulnerabilidad en TCP/IP que odría permitir causar una denegación de servicio (2790655)** | | |
| 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. | | |