**Segmento 99.92.176.0**

### 

**Vulnerabilidades de prioridad Alta para Administración General De Innovación Y Calidad**

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.92.176.230 |

|  |  |  |
| --- | --- | --- |
| **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 KB2286198: Ejecución de código en el análisis del ícono de acceso directo de la Shell de Windows.  MS KB2488013: Internet Explorer no procesa correctamente CSS  MS KB2719662: Vulnerabilidades en Gadgets podría permitir la ejecución de código remoto  MS08-069: Ejecución remota de código sobre Microsoft XML Core Services (955218)  MS09-009: Vulnerabilidades en Microsoft Office Excel podrían permitir ejecución remota de código  MS09-021: Vulnerabilidades en Microsoft Office Excel podrían permitir la ejecución remota de código.  MS09-054: Microsoft Internet Explorer actualización acumulativa de seguridad  MS09-055: Actualización de seguridad acumulativa para ActiveX  MS09-059: Vulnerabilidad en LSSAS (Local Security Authority Subsystem Servic) podría permitir una denegación de servicio  MS09-072: Microsoft Internet Explorer actualización acumulativa de seguridad  MS10-001: OpenType Font Engine permite la ejecución de código remoto  MS10-002: Microsoft Internet Explorer actualización acumulativas de seguridad  MS10-006: Vulnerabilidades en el cliente SMB podrían permitir la ejecución remota de código  MS10-008: Actualización de seguridad acumulativa para ActiveX  MS10-012: Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código  MS10-012: Vulnerabilidades en SMB podrían resultar en ejecución remota de código (971468)  MS10-013: Vulnerabilidad en Microsoft DirectShow podría permitir la ejecución remota de código.  MS10-017: Vulnerabilidades en Microsoft Office Excel podrían permitir la ejecución remota de código (980150)  MS10-018: Actualización de seguridad acumulativa para Internet Explorer  MS10-019: Vulnerabilidades en Windows podrían permitir la ejecución de código (981210)  MS10-020: Vulnerabilidades en SMB Client podrían permitir la ejecución remota de código  MS10-022: Vulnerabilidad en el motor de secuencias de comandos VBScript podría permitir la ejecución remota de código  MS10-030: Vulnerabilidad en Outlook Express y Windows Mail podrían permitir la ejecución remota de código.  MS10-032: Vulnerabilidades en los controladores de Windows Kernel-Mode podrían permitir la elevación de privilegios  MS10-033: Vulnerabilidades en la descompresión de archivos multimedia, podrían permitir la ejecución remota de código(979902)  MS10-034: Actualización de seguridad acumulativa para ActiveX  MS10-035: Actualización de seguridad acumulativa para Internet Explorer  MS10-038: Vulnerabilidades en Microsoft Office Excel podrían permitir la ejecución remota de código(2027452)  MS10-046: Vulnerabilidad en la shell de Windows podría permitir la ejecución remota de código  MS10-047: Vulnerabilidad en el kernel de Windows que podría permitir la elevación de privilegios  MS10-048: Vulnerabilidad en los controladores de Windows en modo kernel-podrían permitir elevación de privilegios  MS10-049: Vulnerabilidad en Schannel que podría permitir la ejecución de código malicioso remotamente, e incluso podría realizar una Denegación de Servicio  MS10-051: Vulnerabilidad en Microsoft XML Core Services permite la ejecución remota de código (2079403)  MS10-053: Actualización de seguridad acumulativa para Internet Explorer  MS10-054: Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código  MS10-054: Vulnerabilidades en SMB Server podrían permitir la ejecución remota de código.  MS10-058: Vulnerabilidades en TCP/IP, podrían permitir la elevación de privilegios (978886)  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  MS10-061: Vulnerabilidad en el servicio Print Spooler (cola de impresión) podría permitir la ejecución remota de código  MS10-071: Actualización de seguridad acumulativa para Internet Explorer  MS10-073: Vulnerabilidad en Windows en donde los controladores a modo kernel, podrían permitir la elevación de privilegios  MS10-074: Vulnerabilidad en Microsoft Foundation Classes podría permitir la ejecución remota de código  MS10-075: Vulnerabilidad en el servicio de Media Player Network Sharing puede permitir ejecución remota de código  MS10-076: Vulnerabilidad en el motor de fuentes OpenType que podría permitir la ejecución de código remotamente  MS10-079: Vulnerabilidades en Microsoft Word podrían permitir la ejecución remota de código (2293194)  MS10-080: Vulnerabilidades en Microsoft Excel podrían permitir la ejecución remota de código (2293211)  MS10-081: Vulnerabilidad en Windows en los controles de librería permita la ejecución remota de código  MS10-082: Vulnerabilidad en Windows Media Player, podría permitir la ejecución remota de código (2378111)  MS10-083: Una vulnerabilidad en la validación COM en el shell de Windows y WordPad, podría permitir la ejecución remota de código (2405882)  MS10-085: Vulnerabilidad en SChannel podría permitir crear una condición de Denegación de Servicio  MS10-087: Microsoft Office puede permitir la ejecución de código remoto  MS10-090: Actualización de seguridad acumulativa para Internet Explorer  MS10-091: Vulnerabilidades en la fuente OpenType (OTF) del controlador podría permitir la ejecución de código remotamente  MS10-092: Vulnerabilidad en el programador de tareas (task scheduler) podría permitir la elevación de privilegios  MS10-095: Vulnerabilidad en Microsoft Windows puede permitir la ejecución remota de código  MS10-096: Vulnerabilidad en Windows Address Book podría permitir la ejecución remota de código  MS10-098: Vulnerabilidad de Elevación de privilegios en el kernel de Windows  MS10-100: Vulnerabilidad en la Interfaz del usuario podría permitir la elevación de privilegios  MS10-103: Microsoft Publisher podría permitir la ejecución código remoto  MS10-105:Vulnerabilidad en Microsoft Office  MS11-002: Vulnerabilidades en Microsoft Data Access Components que podrían permitir la ejecución remota de código  MS11-003: IE Actualización de seguridad acumulativa para Internet Explorer  MS11-007: 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  MS11-015: Vulnerabilidades en Windows Media podrían permitir la ejecución remota de código  MS11-017: Vulnerabilidad en una conexión de escritorio remoto, permitiendo la ejecución de código  MS11-018: Actualización de seguridad acumulativa para Internet Explorer (2497640)  MS11-019: Vulnerabilidades en SMB Client permiten la ejecución de código remoto.  MS11-020: SMB presenta fallas en su implementación que permite la ejecución de código remoto  MS11-020: Vulnerabilidad en SMB server podría resultar en ejecución remota de código (2508429)  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)  MS11-024: Vulnerabilidad en el editor Windows Fax Cover Page permite la ejecución de código remoto.  MS11-025: Vulnerabilidad en la librería Microsoft Foundation Class (MFC), podría permitir la ejecución remota de código (2500212)  MS11-027: Actualización de seguridad acumulativa para ActiveX  MS11-028: Vulnerabilidad en .NET Framework, podría permitir la ejecución de código arbitrario  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.  MS11-034: Vulnerabilidades en los controladores Windows Kernel-Mode, podrían permitir la elevación de privilegios.  MS11-036: Vulnerabilidades en Microsoft PowerPoint podrían permitir ejecutar código remoto (2545814)  MS11-038: Vulnerabilidades en OLE Automation podrían permitir ejecución de código remoto (2476490)  MS11-039: 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)  MS11-045: Vulnerabilidad en Microsoft Excel podría permitir ejecución de código remota (2537146)  MS11-046: Vulnerabilidad en Ancillary Function Driver podría permitir ejecución de código remota (2503665)  MS11-048: Vulnerabilidad en SMB Server podría ocasionar una denegación de servicio (2536275)  MS11-048: Vulnerabilidad en SMB Server podría permitir una denegación de servicio (2536275)  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)  MS11-063 Vulnerabilidad en el subsistema cliente/servidor en tiempo de ejecución podría permitir la elevación de privilegios.  MS11-064: Una vulnerabilidad en la pila TCP / IP podrían permitir la denegación de servicio (2563894)  MS11-068: Una vulnerabilidad en el kernel de Windows podrían permitir la denegación de servicio (2556532)  MS11-071 Vulnerabilidad en componentes de windows podría permitir ejecución de código de manera remota.  MS11-072: Vulnerabilidades en Microsoft Excel podría permitir la ejecución remota de código (2587505)  MS11-073: Vulnerabilidades en Microsoft Office podría permitir ejecución de código remoto (2587634)  MS11-075: Vulnerabilidad en Microsoft Active Accessibility podría permitir la ejecución remota de código (2623699)  MS11-076: Vulnerabilidad en Windows Media Center podría permitir la ejecución remota (2604926)  MS11-077: 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)  MS11-081: Actualización de seguridad acumulativa para Internet Explorer (2586448)  MS11-083: Vulnerabilidad en TCP/IP podría permitir la ejecución remota de código (2588516)  MS11-084: Vulnerabilidad en Windows Kernel-Mode Drivers podría permitir una denegación de servicio (2617657)  MS11-087: Vulnerabilidad en Microsoft en el kernel de Windows podrían permitir la ejecución remota de código  MS11-089: Una vulnerabilidad en Microsoft Office podría permitir la ejecución remota de código  MS11-090: Actualización de seguridad para ActiveX  MS11-092: Una vulnerabilidad en Windows Media podría permitir la ejecución remota de código  MS11-094: Una vulnerabilidad en Microsoft PowerPoint podrían permitir la ejecución remota de código  MS11-097: Una vulnerabilidad en el subsistema de Windows en tiempo de ejecución cliente / servidor podría permitir la elevación 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 políticas de seguridad (2644615)  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)  MS12-010: Actualizaciones de parches de seguridad acumulativos para Internet Explorer (2647516)  MS12-013: Vulnerabilidad en la librería C Run-Time podría permitir la ejecución de código remoto (2654428)  MS12-015: Vulnerabilidades en Microsoft Visio Viewer 2010 podrían permitir ejecución remota de código (2663510)  MS12-016: Vulnerabilidad en .NET Framework y Microsoft Silverlight podrían permitir ejecución de código remoto (2651026)  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)  MS12-029: Vulnerabilidad en Microsoft Word podría ocasionar ejecución remota de código (2680352)  MS12-030: Vulnerabilidad en Microsoft Office podría ocasionar ejecución remota de código (2663830)  MS12-031: Vulnerabilidad en Microsoft Visio Viewer 2010 podría ocasionar ejecución remota de código (2597981)  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 de código remoto (2706726)  MS12-041: Vulnerabilidades en los drivers del Kernel-Mode de Windows podrían permitir la elevación de privilegios (2709162)  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)  MS12-046: Vulnerabilidad en Visual Basic for Applications podría permitir la ejecución de código remoto (2707960)  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)  MS12-064: Vulnerabilidad en Microsoft Word podría permitir la ejecución de código remoto (2742319)  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)  MS12-076: Vulnerabilidad en Microsoft Office podría permitir la ejecución de código remoto (2720184)  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: Vulnerabilidad en DirectPlay podría permitir la ejecución de código remoto (2770660)  MS13-001: Vulnerabilidad en Windows Print Spooler Components podría permitir la ejecución remota de código (2769369)  MS13-002: Vulnerabilidad en Microsoft XML 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 privilegios (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)  MS13-021: Actualizaciones de seguridad para Internet Explorer (2809289)  MS13-027: Vulnerabilidad en Kernel-Mode Drivers podría permitir elevación de privilegios de seguridad (2807986)  MS13-028: Actualización de seguridad para Internet Explorer (2817183)  MS13-029: Vulnerabilidad en Remote Desktop Client podría permitir la ejecución remota de código (2828223)  MS13-031: Vulnerabilidad en el kernel de Windows podría permitir la elevación de privilegios (2813170)  MS13-036: Vulnerabilidad en el Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2829996) | | |
| 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** |
| 99.92.176.29 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS11-020: SMB presenta fallas en su implementación que permite la ejecución de código remoto | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.92.176.32 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS11-020: SMB presenta fallas en su implementación que permite la ejecución de código remoto  MS11-048: Vulnerabilidad en SMB Server podría ocasionar una denegación de servicio (2536275) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.92.176.37 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS11-048: Vulnerabilidad en SMB Server podría ocasionar una denegación de servicio (2536275) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.92.176.48 |

|  |  |  |
| --- | --- | --- |
| **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 KB2719662: Vulnerabilidades en Gadgets podría permitir la ejecución de código remoto  MS08-069: Ejecución remota de código sobre Microsoft XML Core Services (955218)  MS10-012: Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código  MS11-007: Vulnerabilidad en el controlador del OpenType Compact Font Format (CFF) podría permitir la ejecución remota de código  MS11-015: Vulnerabilidades en Windows Media podrían permitir la ejecución remota de código  MS11-019: Vulnerabilidades en SMB Client permiten la ejecución de código remoto.  MS11-020: Vulnerabilidad en SMB server podría resultar en ejecución remota de código (2508429)  MS11-024: Vulnerabilidad en el editor Windows Fax Cover Page permite la ejecución de código remoto.  MS11-027: Actualización de seguridad acumulativa para ActiveX  MS11-030: Vulnerabilidad en la resolución DNS podría permitir la ejecución remota de código  MS11-031: Vulnerabilidad en los motores de scripting de JScript y VBScript podría permitir la ejecución remota de código.  MS11-032: Vulnerabilidad en el controlador OpenType Compact Font Format (CFF) podría permitir la ejecución remota de código.  MS11-038: Vulnerabilidades en OLE Automation podrían permitir ejecución de código remoto (2476490)  MS11-043: Una vulnerabilidad en el cliente SMB podrían permitir la ejecución remota de código (2536276)  MS11-046: Vulnerabilidad en Ancillary Function Driver podría permitir ejecución de código remota (2503665)  MS11-048: Vulnerabilidad en SMB Server podría ocasionar una denegación de servicio (2536275)  MS11-048: Vulnerabilidad en SMB Server podría permitir una denegación de servicio (2536275)  MS11-071 Vulnerabilidad en componentes de windows podría permitir ejecución de código de manera remota.  MS11-075: Vulnerabilidad en Microsoft Active Accessibility podría permitir la ejecución remota de código (2623699)  MS11-076: Vulnerabilidad en Windows Media Center podría permitir la ejecución remota (2604926)  MS11-090: Actualización de seguridad para ActiveX  MS11-092: Una vulnerabilidad en Windows Media podría permitir la ejecución remota de código  MS11-097: Una vulnerabilidad en el subsistema de Windows en tiempo de ejecución cliente / servidor podría permitir la elevación de privilegios  MS12-039: Vulnerabilidad en Lync podría permitir la ejecución de código remoto (2707956)  MS12-074: Vulnerabilidad en .NET Framework podría permitir la ejecución de código remoto (2745030)  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  MS12-079: Vulnerabilidad en Microsoft Word podría permitir la ejecución remota de código (2780642)  MS12-082: Vulnerabilidad en DirectPlay podría permitir la ejecución de código remoto (2770660)  MS13-001: Vulnerabilidad en Windows Print Spooler Components podría permitir la ejecución remota de código (2769369)  MS13-002: Vulnerabilidad en Microsoft XML podría permitir la ejecución de código remoto (2756145)  MS13-022: Vulnerabilidad en Microsoft Silverlight podría permitir ejecución de código remoto (2814124)  MS13-028: Actualización de seguridad para Internet Explorer (2817183)  MS13-029: Vulnerabilidad en Remote Desktop Client podría permitir la ejecución remota de código (2828223)  MS13-031: Vulnerabilidad en el kernel de Windows podría permitir la elevación de privilegios (2813170)  MS13-036: Vulnerabilidad en el Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2829996) | | |
| 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** |
| 99.92.176.5 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS11-020: SMB presenta fallas en su implementación que permite la ejecución de código remoto | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.92.176.58 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS11-020: SMB presenta fallas en su implementación que permite la ejecución de código remoto | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.92.176.60 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2695962: Actualización para ActiveX en sus Kill Bits (2695962)  MS KB2719662: Vulnerabilidades en Gadgets podría permitir la ejecución de código remoto  MS08-069: Ejecución remota de código sobre Microsoft XML Core Services (955218)  MS11-007: Vulnerabilidad en el controlador del OpenType Compact Font Format (CFF) podría permitir la ejecución remota de código  MS11-015: Vulnerabilidades en Windows Media podrían permitir la ejecución remota de código  MS11-019: Vulnerabilidades en SMB Client permiten la ejecución de código remoto.  MS11-020: Vulnerabilidad en SMB server podría resultar en ejecución remota de código (2508429)  MS11-024: Vulnerabilidad en el editor Windows Fax Cover Page permite la ejecución de código remoto.  MS11-027: Actualización de seguridad acumulativa para ActiveX  MS11-030: Vulnerabilidad en la resolución DNS podría permitir la ejecución remota de código  MS11-031: Vulnerabilidad en los motores de scripting de JScript y VBScript podría permitir la ejecución remota de código.  MS11-032: Vulnerabilidad en el controlador OpenType Compact Font Format (CFF) podría permitir la ejecución remota de código.  MS11-038: Vulnerabilidades en OLE Automation podrían permitir ejecución de código remoto (2476490)  MS11-043: Una vulnerabilidad en el cliente SMB podrían permitir la ejecución remota de código (2536276)  MS11-046: Vulnerabilidad en Ancillary Function Driver podría permitir ejecución de código remota (2503665)  MS11-048: Vulnerabilidad en SMB Server podría permitir una denegación de servicio (2536275)  MS11-071 Vulnerabilidad en componentes de windows podría permitir ejecución de código de manera remota.  MS11-075: Vulnerabilidad en Microsoft Active Accessibility podría permitir la ejecución remota de código (2623699)  MS11-076: Vulnerabilidad en Windows Media Center podría permitir la ejecución remota (2604926)  MS11-085: Vulnerabilidad en Windows Mail and Windows Meeting Space podría permitir la ejecución remota de código (2620704)  MS11-090: Actualización de seguridad para ActiveX  MS11-092: Una vulnerabilidad en Windows Media podría permitir la ejecución remota de código  MS11-097: Una vulnerabilidad en el subsistema de Windows en tiempo de ejecución cliente / servidor podría permitir la elevación de privilegios  MS12-039: Vulnerabilidad en Lync podría permitir la ejecución de código remoto (2707956)  MS12-074: Vulnerabilidad en .NET Framework podría permitir la ejecución de código remoto (2745030)  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  MS12-079: Vulnerabilidad en Microsoft Word podría permitir la ejecución remota de código (2780642)  MS12-082: Vulnerabilidad en DirectPlay podría permitir la ejecución de código remoto (2770660)  MS13-022: Vulnerabilidad en Microsoft Silverlight podría permitir ejecución de código remoto (2814124)  MS13-028: Actualización de seguridad para Internet Explorer (2817183)  MS13-029: Vulnerabilidad en Remote Desktop Client podría permitir la ejecución remota de código (2828223)  MS13-031: Vulnerabilidad en el kernel de Windows podría permitir la elevación de privilegios (2813170)  MS13-036: Vulnerabilidad en el Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2829996) | | |
| 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** |
| 99.92.176.62 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS11-048: Vulnerabilidad en SMB Server podría ocasionar una denegación de servicio (2536275) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.92.176.63 |

|  |  |  |
| --- | --- | --- |
| **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  MS11-020: SMB presenta fallas en su implementación que permite la ejecución de código remoto  MS11-048: Vulnerabilidad en SMB Server podría ocasionar una denegación de servicio (2536275) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.92.176.66 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2695962: Actualización para ActiveX en sus Kill Bits (2695962)  MS KB2719662: Vulnerabilidades en Gadgets podría permitir la ejecución de código remoto  MS08-069: Ejecución remota de código sobre Microsoft XML Core Services (955218)  MS10-012: Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código  MS11-007: Vulnerabilidad en el controlador del OpenType Compact Font Format (CFF) podría permitir la ejecución remota de código  MS11-015: Vulnerabilidades en Windows Media podrían permitir la ejecución remota de código  MS11-019: Vulnerabilidades en SMB Client permiten la ejecución de código remoto.  MS11-020: SMB presenta fallas en su implementación que permite 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.  MS11-025: Vulnerabilidad en la librería Microsoft Foundation Class (MFC), podría permitir la ejecución remota de código (2500212)  MS11-027: Actualización de seguridad acumulativa para ActiveX  MS11-030: Vulnerabilidad en la resolución DNS podría permitir la ejecución remota de código  MS11-031: Vulnerabilidad en los motores de scripting de JScript y VBScript podría permitir la ejecución remota de código.  MS11-032: Vulnerabilidad en el controlador OpenType Compact Font Format (CFF) podría permitir la ejecución remota de código.  MS11-038: Vulnerabilidades en OLE Automation podrían permitir ejecución de código remoto (2476490)  MS11-043: Una vulnerabilidad en el cliente SMB podrían permitir la ejecución remota de código (2536276)  MS11-046: Vulnerabilidad en Ancillary Function Driver podría permitir ejecución de código remota (2503665)  MS11-048: Vulnerabilidad en SMB Server podría ocasionar una denegación de servicio (2536275)  MS11-048: Vulnerabilidad en SMB Server podría permitir una denegación de servicio (2536275)  MS11-059: Una vulnerabilidad en el componente Microsoft Data Access podría permitir la ejecución remota de código (2560656)  MS11-071 Vulnerabilidad en componentes de windows podría permitir ejecución de código de manera remota.  MS11-075: Vulnerabilidad en Microsoft Active Accessibility podría permitir la ejecución remota de código (2623699)  MS11-076: Vulnerabilidad en Windows Media Center podría permitir la ejecución remota (2604926)  MS11-085: Vulnerabilidad en Windows Mail and Windows Meeting Space podría permitir la ejecución remota de código (2620704)  MS11-090: Actualización de seguridad para ActiveX  MS11-092: Una vulnerabilidad en Windows Media podría permitir la ejecución remota de código  MS11-097: Una vulnerabilidad en el subsistema de Windows en tiempo de ejecución cliente / servidor podría permitir la elevación de privilegios  MS12-074: Vulnerabilidad en .NET Framework podría permitir la ejecución de código remoto (2745030)  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  MS12-079: Vulnerabilidad en Microsoft Word podría permitir la ejecución remota de código (2780642)  MS12-081: Vulnerabilidad en Windows en el componente de manejo de archivos podría permitir la ejecución de código remoto (2758857)  MS13-001: Vulnerabilidad en Windows Print Spooler Components podría permitir la ejecución remota de código (2769369)  MS13-002: Vulnerabilidad en Microsoft XML podría permitir la ejecución de código remoto (2756145)  MS13-004: Vulnerabilidad en .NET Framework podría permitir la elevación de privilegios (2769324)  MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113)  MS13-022: Vulnerabilidad en Microsoft Silverlight podría permitir ejecución de código remoto (2814124)  MS13-028: Actualización de seguridad para Internet Explorer (2817183)  MS13-029: Vulnerabilidad en Remote Desktop Client podría permitir la ejecución remota de código (2828223)  MS13-031: Vulnerabilidad en el kernel de Windows podría permitir la elevación de privilegios (2813170)  MS13-036: Vulnerabilidad en el Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2829996) | | |
| 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** |
| 99.92.176.68 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS11-048: Vulnerabilidad en SMB Server podría ocasionar una denegación de servicio (2536275) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.92.176.73 |

|  |  |  |
| --- | --- | --- |
| **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 KB2719662: Vulnerabilidades en Gadgets podría permitir la ejecución de código remoto  MS08-069: Ejecución remota de código sobre Microsoft XML Core Services (955218)  MS11-007: Vulnerabilidad en el controlador del OpenType Compact Font Format (CFF) podría permitir la ejecución remota de código  MS11-015: Vulnerabilidades en Windows Media podrían permitir la ejecución remota de código  MS11-019: Vulnerabilidades en SMB Client permiten la ejecución de código remoto.  MS11-020: Vulnerabilidad en SMB server podría resultar en ejecución remota de código (2508429)  MS11-024: Vulnerabilidad en el editor Windows Fax Cover Page permite la ejecución de código remoto.  MS11-027: Actualización de seguridad acumulativa para ActiveX  MS11-030: Vulnerabilidad en la resolución DNS podría permitir la ejecución remota de código  MS11-031: Vulnerabilidad en los motores de scripting de JScript y VBScript podría permitir la ejecución remota de código.  MS11-032: Vulnerabilidad en el controlador OpenType Compact Font Format (CFF) podría permitir la ejecución remota de código.  MS11-038: Vulnerabilidades en OLE Automation podrían permitir ejecución de código remoto (2476490)  MS11-043: Una vulnerabilidad en el cliente SMB podrían permitir la ejecución remota de código (2536276)  MS11-046: Vulnerabilidad en Ancillary Function Driver podría permitir ejecución de código remota (2503665)  MS11-048: Vulnerabilidad en SMB Server podría ocasionar una denegación de servicio (2536275)  MS11-048: Vulnerabilidad en SMB Server podría permitir una denegación de servicio (2536275)  MS11-059: Una vulnerabilidad en el componente Microsoft Data Access podría permitir la ejecución remota de código (2560656)  MS11-071 Vulnerabilidad en componentes de windows podría permitir ejecución de código de manera remota.  MS11-075: Vulnerabilidad en Microsoft Active Accessibility podría permitir la ejecución remota de código (2623699)  MS11-076: Vulnerabilidad en Windows Media Center podría permitir la ejecución remota (2604926)  MS11-085: Vulnerabilidad en Windows Mail and Windows Meeting Space podría permitir la ejecución remota de código (2620704)  MS11-090: Actualización de seguridad para ActiveX  MS11-092: Una vulnerabilidad en Windows Media podría permitir la ejecución remota de código  MS11-097: Una vulnerabilidad en el subsistema de Windows en tiempo de ejecución cliente / servidor podría permitir la elevación de privilegios  MS12-039: Vulnerabilidad en Lync podría permitir la ejecución de código remoto (2707956)  MS12-074: Vulnerabilidad en .NET Framework podría permitir la ejecución de código remoto (2745030)  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  MS12-082: Vulnerabilidad en DirectPlay podría permitir la ejecución de código remoto (2770660)  MS13-022: Vulnerabilidad en Microsoft Silverlight podría permitir ejecución de código remoto (2814124)  MS13-028: Actualización de seguridad para Internet Explorer (2817183)  MS13-029: Vulnerabilidad en Remote Desktop Client podría permitir la ejecución remota de código (2828223)  MS13-031: Vulnerabilidad en el kernel de Windows podría permitir la elevación de privilegios (2813170)  MS13-036: Vulnerabilidad en el Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2829996) | | |
| 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** |
| 99.92.176.74 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS11-048: Vulnerabilidad en SMB Server podría ocasionar una denegación de servicio (2536275) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.92.176.76 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS11-020: SMB presenta fallas en su implementación que permite la ejecución de código remoto  MS11-048: Vulnerabilidad en SMB Server podría ocasionar una denegación de servicio (2536275) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.92.176.230 |

|  |  |  |
| --- | --- | --- |
| **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 podrían 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  MS09-056: Vulnerabilidades en Windows CryptoAPI podrían permitir suplantación de identidad (spoofing)  MS10-015: Vulnerabilidad en el kernel de Windows podría permitir la elevación de privilegios  MS10-021: Vulnerabilidades en el Kernel de Windows podrían permitir la elevación de privilegios.  MS10-037: Vulnerabilidad en el formato OpenType Fuente Compacto (CFF) El controlador podría permitir la elevación de privilegios  MS10-041: Vulnerabilidad en Microsoft .Net Framework que podría permitir falsificaciones (981343)  MS10-070: Vulnerabilidad en ASP.NET podría permitir la revelación de información (2418042)  MS11-009: Vulnerabilidad los motores de scripting de JScript y VBScript podrían permitir la divulgación de información  MS11-026: Vulnerabilidad en MHTML podría permitir la divulgación de información  MS11-037: Múltiples Vulnerabilidades en MHTML podrían permitir revelación de información (2544893)  MS11-056 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)  MS12-006: 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)  MS12-019: Vulnerabilidad en DirectWrite podría permitir una denegación de servicio (2665364)  MS12-032: Vulnerabilidad en TCP/IP podría ocasionar ejecución remota de código (2688338)  MS12-033: Vulnerabilidad en Windows Partition Manager podría ocasionar elevación de privilegios (2690533)  MS12-049: Vulnerabilidad en TLS podría revelar información sensible (2655992)  MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)  MS12-069: Vulnerabilidad en Kerberos podría ocasionar una denegación de servicio (2743555)  MS13-006: Vulnerabilidad en Microsoft Windows podría permitir la evasión de restricciones de seguridad (2785220)  MS13-007: Vulnerabilidad en Open Data Protocol podría permitir una denegación de servicio (2769327)  MS13-018: Vulnerabilidad en TCP/IP que podría permitir causar una denegación de servicio (2790655) | | |
| 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** |
| 99.92.176.48 |

|  |  |  |
| --- | --- | --- |
| **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  MS11-009: Vulnerabilidad los motores de scripting de JScript y VBScript podrían permitir la divulgación de información  MS11-026: Vulnerabilidad en MHTML podría permitir la divulgación de información  MS11-037: Múltiples Vulnerabilidades en MHTML podrían permitir revelación de información (2544893)  MS11-066: Una vulnerabilidad en el control Microsoft Chart podría permitir la divulgación de información  MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)  MS13-006: Vulnerabilidad en Microsoft Windows podría permitir la evasión de restricciones de seguridad (2785220)  MS13-007: Vulnerabilidad en Open Data Protocol podría permitir una denegación de servicio (2769327) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.92.176.60 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Medio / CVSS Base Score : 6.4  (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS 2647518: Actualización para ActiveX Kill Bits (2647518)  MS KB2728973: Certificados digitales no autorizados podrían permitir la suplantación de identidad  MS11-009: Vulnerabilidad los motores de scripting de JScript y VBScript podrían permitir la divulgación de información  MS11-026: Vulnerabilidad en MHTML podría permitir la divulgación de información  MS11-037: Múltiples Vulnerabilidades en MHTML podrían permitir revelación de información (2544893)  MS11-066: Una vulnerabilidad en el control Microsoft Chart podría permitir la divulgación de información  MS13-007: Vulnerabilidad en Open Data Protocol podría permitir una denegación de servicio (2769327) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.92.176.66 |

|  |  |  |
| --- | --- | --- |
| **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)  MS11-009: Vulnerabilidad los motores de scripting de JScript y VBScript podrían permitir la divulgación de información  MS11-026: Vulnerabilidad en MHTML podría permitir la divulgación de información  MS11-066: Una vulnerabilidad en el control Microsoft Chart podría permitir la divulgación de información  MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)  MS13-007: Vulnerabilidad en Open Data Protocol podría permitir una denegación de servicio (2769327) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.92.176.73 |

|  |  |  |
| --- | --- | --- |
| **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 KB2728973: Certificados digitales no autorizados podrían permitir la suplantación de identidad  MS11-009: Vulnerabilidad los motores de scripting de JScript y VBScript podrían permitir la divulgación de información  MS11-026: Vulnerabilidad en MHTML podría permitir la divulgación de información  MS11-037: Múltiples Vulnerabilidades en MHTML podrían permitir revelación de información (2544893)  MS11-066: Una vulnerabilidad en el control Microsoft Chart podría permitir la divulgación de información  MS13-007: Vulnerabilidad en Open Data Protocol podría permitir una denegación de servicio (2769327) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |