**Segmento 99.40.24.0**

### 

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

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.24.125 |

|  |  |  |
| --- | --- | --- |
| **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 KB2219475: Windows Help Center hcp: / / el controlador de protocolo permite la ejecución de código arbitrario  MS KB2269637: Carga insegura de librerías podría permitir ejecución remota de código  MS KB2488013: Internet Explorer no procesa correctamente CSS  MS KB953839: ActiveX Kill Bits actualizaciones de seguridad acumuladas  MS KB955759: Mejoras de seguridad para Indeo Codec  MS KB956391: ActiveX Kill Bits actualización de seguridad acumuladas  MS KB960715: Actualización de seguridad acumulativa para ActiveX  MS KB969898: ActiveX Kill Bits actualización de seguridad acumuladas  MS07-023: Vulnerabilidad en Microsoft Excel  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  MS08-031: Actualización de parches de Seguridad acumulativos para Internet Explorer (950759)  MS08-033: Vulnerabilidad en DirectX podría pemritir ejecución de código remoto (951698)  MS08-036: Vulnerabilidades en Pragmatic General Multicast (PGM) podría permitir una denegación de servicio (950762)  MS08-043: Vulnerabilidad en Microsoft Excel  MS08-045: Actualizaciones de parches de Seguridad acumulativos para Internet Explorer (953838)  MS08-046: Vulnerabilidades en Microsoft Windows Image Color Management System podría permitir ejecución de código remoto (952954)  MS08-049: Vulnerabilidades en Event System podría permitir la ejecución remota de código (950974)  MS08-051: Vulnerabilidad en Microsoft PowerPoint  MS08-052: Vulnerabilidades en GDI+ podrían permitir la ejecución remota de código  MS08-055: Vulnerabilidad en Microsoft Office  MS08-058: Múltiples vulnerabilidades en Microsoft Internet Explorer (956390)  MS08-061: Múltiples problemas de elevación de privilegios en Microsoft Windows Kernel (954211)  MS08-063: Desbordamiento de búfer en el manejo de archivos SMB en Microsoft Windows (957095)  MS08-064: Elevación de privilegios locales en Microsoft Windows Virtual Address Descriptors (VAD) (956841)  MS08-066: Elevación de privilegios en Microsoft Windows Ancillary Function Driver (afd.sys) (956803)  MS08-067: Manejo inseguro de solicitudes en Microsoft Windows Server Service Crafted RPC podría permitir ejecución remota de código (958644)  MS08-068: Vulnerabilidad en SMB podría permitir ejecución de código remoto(957097)  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  MS08-071: Vulnerabilidades en GDI+ podría permitir ejecución de cpodigo remoto (956802)  MS08-073: Múltiples vulnerabilidades en Microsoft Internet Explorer (958215)  MS08-076: Vulnerabilidades en Windows Media Components podría permitir ejecución remota de código (959807)  MS08-078: Actualizaciones de Seguridad para Microsoft Internet Explorer (960714)  MS09-001: Vulnerabilidades en SMB podrían permitir la ejecución de código remoto  MS09-006: Vulnerabilidades en Windows Kernel podrían permitir ejecución de código (958690)  MS09-009: Vulnerabilidades en Microsoft Office Excel podrían permitir ejecucion remota de codigo  MS09-011: Microsoft DirectShow presenta una vulnerabilidad en podría permitir la ejecución de código remoto  MS09-012: Vulnerabilidades en Windows podrían permitir elevación de privilegios (959454)  MS09-013: Vulnerabilidades en Windows HTTP Services podrían permitir ejecución remota de código (960803)  MS09-014: Actualizaciones de seguridad acumulativas para Internet Explorer (963027)  MS09-019: Actualizaciones de seguridad acumulativas para Internet Explorer (969897)  MS09-021: Vulnerabilidades en Microsoft Office Excel podrían permitir la ejecución remota de código.  MS09-022: Windows Print Spooler presenta vulnerabilidades podría permitir la ejecución de código remoto  MS09-025: Vulnerabilidades en el Kernel de Windows podría permitir la elevación de privilegios (968537)  MS09-026: Vulnerabilidad en RPC podría permitir la elevación de privilegios (970238)  MS09-027: Vulnerabilidades en Microsoft Office Word podrían permitir la ejecucion remota de codigo  MS09-028: Vulnerabilidades en Microsoft DirectShow podrían permitir ejecución remota de código (971633)  MS09-029: Vulnerabilidades en el motor de fuentes OpenType incrustadas podrían permitir la ejecución remota de código  MS09-030: Vulnerabilidad en Microsoft Office Publisher podría permitir la ejecución de código remoto (969516)  MS09-032: ActiveX Kill Bits actualización de seguridad acumulada  MS09-034: Parches Acumulativos de Actualizaciones de Seguridad para Internet Explorer (972260)  MS09-037: Microsoft Active Témplate Library (ATL) presenta una vulnerabilidad que permite la ejecución de código remoto  MS09-038: Vulnerabilidad en Windows Media File Processing permite la ejecución remota de código (971557)  MS09-041: Vulnerabilidad en Workstation Service podría permitir elevación de privilegios (971657)  MS09-042: Vulnerabilidad en Telnet podría permitir ejecución remota de código (960859)  MS09-044: Vulnerabilidad en la conexión de escritorio remoto podría permitir la ejecución remota de código  MS09-045: Vulnerabilidad en Jscript Scripting Engine que permite ejecución remota de código (971961)  MS09-047: Vulnerabilidades en el formato de Windows Media podría permitir la ejecución remota de código (973812)  MS09-051: Windows Media Runtime presenta vulnerabilidades podría permitir la ejecución de código remoto  MS09-052: Windows Media Player presenta vulnerabilidad podría permitir la ejecución de código remoto  MS09-054: Microsoft Internet Explorer actualización acumulativa de seguridad  MS09-055: Actualización de seguridad acumulativa para ActiveX  MS09-057: Indexing Service permite la ejecución de código remoto  MS09-058: Windows Kernel podría permitir elevación de privilegios  MS09-060: Vulnerabilidades en Controles ActiveX de Microsoft Active Template Library (ATL) para Microsoft Office podrían permitir la ejecución remota de código (973965)  MS09-065: Vulnerabilidades en controladores del Kernel-Mode de Windows podría permitir la ejecución remota de código (969947)  MS09-071: Vulnerabilidades en Internet Authentication Service podría permitir la ejecución remota de código  MS09-072: Microsoft Internet Explorer actualización acumulativa de seguridad  MS09-073: Vulnerabilidad en WordPad y Office Text Converters podría permitir la ejecución remota de código (975539)  MS10-001: OpenType Font Engine permite la ejecución de código remoto  MS10-002: Microsoft Internet Explorer actualización acumulativas de seguridad  MS10-005: Microsoft Paint permite la ejecución de código remotamente  MS10-006: Vulnerabilidades en el cliente SMB podrían permitir la ejecución remota de código  MS10-007: Windows Shell presenta una vulnerabilidad podría permitir la ejecución de código remoto  MS10-008: Actualización de seguridad acumulativa para ActiveX  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.  MS10-016: Windows Movie Maker permite la ejecución de código remoto  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  MS10-023: Vulnerabilidad en Microsoft Office Publisher podría permitir la ejecucion remota de codigo  MS10-026: Microsoft MPEG Layer-3 codecs permite la ejecución de código remoto  MS10-027: Windows Media Player permite la ejecución de código remoto  MS10-030: Vulnerabilidad en Outlook Express y Windows Mail podrían permitir la ejecución remota de código.  MS10-031: Vulnerabilidad en Microsoft Visual Basic para aplicaciones podría 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  MS10-036: 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)  MS10-042: Vulnerabilidad en el Centro de ayuda y soporte técnico podría permitir la ejecución de código remoto  MS10-045: Vulnerabilidad en Microsoft Outlook  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  MS10-050: Vulnerabilidad en Windows Movie Maker podría permitir ejecución remota de código (981997)  MS10-051: Vulnerabilidad en Microsoft XML Core Services permíte la ejecución remota de código (2079403)  MS10-052: Vulnerabilidad en Microsoft MPEG Layer-3 Codeds podría permitir la ejecución remota de código (2115168)  MS10-053: Actualización de seguridad acumulativa para Internet Explorer  MS10-054: Vulnerabilidades en SMB Server podrían permitir la ejecución remota de código.  MS10-055: Vulnerabilidad en códec multimedia Cinepak podría permitir la ejecución remota de código (982665)  MS10-061: Vulnerabilidad en el servicio Print Spooler (cola de impresión) podría permitir la ejecución remota de código  MS10-062: Vulnerabilidad en MPEG-4 Codec podría permitir ejecución de código remota (975558)  MS10-066: Vulnerabilidad en Remote Procedure Call podría ejecutar código arbitrario (982802)  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  MS10-076: Vulnerabilidad en el motor de fuentes OpenType que podría permitir la ejecución de código remotamente  MS10-078: Múltiples vulnerabilidades en el controlador de formato de tipo de fuente OpenType (OTF) puede permitir la elevación de privilegios  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)  MS10-084: Una vulnerabilidad en Windows local procedure call, podría permitir la elevación de privilegios (2360937)  MS10-088: Vulnerabilidades en Microsoft PowerPoint podrían permitir la ejecución remota de código (2293386)  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  MS10-096: Vulnerabilidad en Windows Address Book podría permitir la ejecución remota de código  MS10-097: Carga insegura de librerías en Internet Connection Signup Wizard podría permitir ejecución remota de código (2443105)  MS10-098: Vulnerabilidad de Elevación de privilegios en el kernel de Windows  MS10-099: Vulnerabilidad en Routing and Remote Access podría permitir elevación de privilegios (2440591)  MS10-103: Microsoft Publisher podría permitir la ejecución código remoto  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  MS11-014: Vulnerabilidad en Local Security Authority Subsystem Service podría permitir elevación de privilegios localmente (2478960)  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: 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.  MS11-027: 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.  MS11-034: 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)  MS11-042: 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)  MS11-046: 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.  MS11-072: Vulnerabilidades en Microsoft Excel podría permitir la ejecución remota de código (2587505)  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)  MS11-080: 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  MS11-091: Vulnerabilidad en Microsoft Publisher podría permitir la ejecución remota de código  MS11-092: Una vulnerabilidad en Windows Media podría permitir la ejecución remota de código  MS11-093: Vulnerabilidad en OLE podría permitir ejecución de código remoto(2624667)  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 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  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)  MS12-010: Actualizaciones de parches de seguridad acumulativos para Internet Explorer (2647516)  MS12-014: Vulnerabilidad en Indeo Codec podría permitir la ejecución de código remoto (2661637)  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)  MS12-027: 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)  MS12-034: Actualizaciones de Seguridad para Microsoft Office, Windows, .NET Framework, y Silverlight (2681578)  MS12-036: Vulnerabilidad en Remote Desktop podría permitir la ejecución de código remoto (2685939)  MS12-037: Actualización acumulativa de seguridad para Internet Explorer (2699988)  MS12-041: 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)  MS12-046: 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)  MS12-052: Actualizaciones de seguridad acumulativas para Internet Explorer (2722913)  MS12-053: Vulnerabilidad en Remote Desktop podría permitir la ejecución remota de código (2723135)  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)  MS12-075: 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)  MS12-082: 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)  MS13-008: 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)  MS13-016: 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)  MS13-020: Vulnerabilidad en OLE Automation podría permitir la ejecución remota de código (2802968)  MS13-021: Actualizaciones de seguridad para Internet Explorer (2809289)  MS13-027: Vulnerabilidad en Kernel-Mode Drivers podría permitir elevación de privilegios de seguridad (2807986) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.24.166 |

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

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.24.168 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS10-012: Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.24.252 |

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

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.24.53 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  CVSS Base Score : 10.0  (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto carece de múltiples actualizaciones de seguridad de sistema operativo; la falta de estas resulta un riesgo para Confidencialidad, Integridad y Disponibilidad de la información resguardada. |
| **Lista de Actualizaciones:**  MS10-012: Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.24.81 |

|  |  |  |
| --- | --- | --- |
| **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  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)  MS11-090: ActualizaciÃ³n de seguridad para ActiveX  MS11-092: Una vulnerabilidad en Windows Media podría permitir la ejecución remota de código  MS11-097: Una vulnerabilidad en el subsistema de Windows en tiempo de ejecuciÃ³n cliente / servidor podrÃ­a permitir la elevaciÃ³n de privilegios  "MS12-074: Vulnerabilidad en .NET Framework podría permitir la ejecución de código remoto (2745030)  "  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  MS12-082: Vulnerabiloidad en DirectPlay podría permitir la ejecución de código remoto (2770660)  MS13-001: Vulnerabilidad en Windows Print Spooler Components podría permitir la ejecución remota de código (2769369)  MS13-002: Vulnerabilidad en Microsoft XML podria permitir la ejecución de código remoto (2756145)  MS13-004: Vulnerabilidad en .NET Framework podría permitir la elevación de privilegios (2769324)  MS13-021: Actualizaciones de seguridad para Internet Explorer (2809289)  MS13-022: Vulnerabilidad en Microsoft Silverlight podría permitir ejecución de código remoto (2814124)  MS13-027: Vulnerabilidad en Kernel-Mode Drivers podría permitir elevación de privilegios de seguridad (2807986) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.24.86 |

|  |  |  |
| --- | --- | --- |
| **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 KB2219475: Windows Help Center hcp: / / el controlador de protocolo permite la ejecución de código arbitrario  MS KB2269637: Carga insegura de librerías podría permitir ejecución remota de código  MS KB2488013: Internet Explorer no procesa correctamente CSS  MS07-023: Vulnerabilidad en Microsoft Excel  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  MS08-026: Vulnerabilidad en Microsoft Word  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  MS08-072: Vulnerabilidad en Microsoft Word  MS09-009: Vulnerabilidades en Microsoft Office Excel podrían permitir ejecucion remota de codigo  MS09-019: Actualizaciones de seguridad acumulativas para Internet Explorer (969897)  MS09-021: Vulnerabilidades en Microsoft Office Excel podrían permitir la ejecución remota de código.  MS09-023: Vulnerabilidad en Windows Search podría permitir la revelación de información sensible (963093)  MS09-030: Vulnerabilidad en Microsoft Office Publisher podría permitir la ejecución de código remoto (969516)  MS09-034: Parches Acumulativos de Actualizaciones de Seguridad para Internet Explorer (972260)  MS09-045: Vulnerabilidad en Jscript Scripting Engine que permite ejecución remota de código (971961)  MS09-054: Microsoft Internet Explorer actualización acumulativa de seguridad  MS09-060: Vulnerabilidades en Controles ActiveX de Microsoft Active Template Library (ATL) para Microsoft Office podrían permitir la ejecución remota de código (973965)  MS09-072: Microsoft Internet Explorer actualización acumulativa de seguridad  MS10-002: Microsoft Internet Explorer actualización acumulativas de seguridad  MS10-005: Microsoft Paint permite la ejecución de código remotamente  MS10-017: Vulnerabilidades en Microsoft Office Excel podrían permitir la ejecución remota de código (980150)  MS10-018: Actualización de seguridad acumulativa para Internet Explorer  MS10-022: Vulnerabilidad en el motor de secuencias de comandos VBScript podría permitir la ejecución remota de código  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)  MS10-035: Actualización de seguridad acumulativa para Internet Explorer  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)  MS10-042: Vulnerabilidad en el Centro de ayuda y soporte técnico podría permitir la ejecución de código remoto  MS10-045: Vulnerabilidad en Microsoft Outlook  MS10-049: Vulnerabilidad en Schannel que podría permitir la ejecución de código malicioso remotamente, e incluso podría realizar una Denegación de Servicio  MS10-050: Vulnerabilidad en Windows Movie Maker podría permitir ejecución remota de código (981997)  MS10-051: Vulnerabilidad en Microsoft XML Core Services permíte la ejecución remota de código (2079403)  MS10-052: Vulnerabilidad en Microsoft MPEG Layer-3 Codeds podría permitir la ejecución remota de código (2115168)  MS10-053: Actualización de seguridad acumulativa para Internet Explorer  MS10-055: Vulnerabilidad en códec multimedia Cinepak podría permitir la ejecución remota de código (982665)  MS10-060:. Vulnerabilidades en Microsoft NET Common Language Runtime y en Microsoft Silverlight de podrían permitir la ejecución remota de código  MS10-071: Actualización de seguridad acumulativa para Internet Explorer  MS10-080: Vulnerabilidades en Microsoft Excel podrían permitir la ejecución remota de código (2293211)  MS10-088: Vulnerabilidades en Microsoft PowerPoint podrían permitir la ejecución remota de código (2293386)  MS10-090: Actualización de seguridad acumulativa para Internet Explorer  MS10-103: Microsoft Publisher podría permitir la ejecución código remoto  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)  MS11-016: Vulnerabilidad en Microsoft Groove podría permitir la ejecución remota de código (249447)  MS11-018: Actualización de seguridad acumulativa para Internet Explorer (2497640)  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)  MS11-028: Vulnerabilidad en .NET Framework, podría permitir la ejecución de código arbitrario  MS11-031: Vulnerabilidad en los motores de scripting de JScript y VBScript podría permitir la ejecución remota de código.  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)  MS11-050: 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.  MS11-072: Vulnerabilidades en Microsoft Excel podría permitir la ejecución remota de código (2587505)  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)  MS11-081: 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  MS11-091: Vulnerabilidad en Microsoft Publisher podría permitir la ejecución remota de código  MS11-092: Una vulnerabilidad en Windows Media podría permitir la ejecución remota de código  MS11-093: Vulnerabilidad en OLE podría permitir ejecución de código remoto(2624667)  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 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)  MS12-002: 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)  MS12-010: Actualizaciones de parches de seguridad acumulativos para Internet Explorer (2647516)  MS12-014: Vulnerabilidad en Indeo Codec podría permitir la ejecución de código remoto (2661637)  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)  MS12-030: Vulnerabilidad en Microsoft Office podría ocasionar ejecución remota de código (2663830)  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)  MS12-046: 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)  MS12-053: Vulnerabilidad en Remote Desktop podría permitir la ejecución remota de código (2723135)  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)  MS12-076: 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: 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)  MS13-020: Vulnerabilidad en OLE Automation podría permitir la ejecución remota de código (2802968)  MS13-021: Actualizaciones de seguridad para Internet Explorer (2809289)  MS13-027: Vulnerabilidad en Kernel-Mode Drivers podría permitir elevación de privilegios de seguridad (2807986) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.24.125 |

|  |  |  |
| --- | --- | --- |
| **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 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  MS08-032: Actualización de parches de seguridad acumulativos para ActiveX Kill Bits (950760)  MS08-037: Vulnerabilidad en DNS podría permitir suplantación de identidad (953230)  MS08-048: Outlook Express y Windows Mail, actualización de seguridad  MS08-050: Windows Messenger presenta vulnerabilidades podría permitir revelar información sensible  MS09-007: Vulnerabilidad en Schannel podría permitir la Falsificación de credenciales de usuario  MS09-015: Vulnerabilidad en SearchPath cuenta con diferentes vulnerabilidades mixtas cuales pueden permitir la elevación de privilegios  MS09-056: Vulnerabilidades en Windows CryptoAPI podrían permitir suplantación de identidad (spoofing)  MS09-069: Vulnerabilidad en Local Security Authority Subsystem Service podría permitir una denegación de servicio (974392)  MS10-011: Windows Client/Server Run-time Subsystem que permite la elevación de privilegios  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.  MS10-029: Windows ISATAP presenta una vulnerabilidad en su componente que podría permitir la suplantación de identidad  MS10-037: Vulnerabilidad en el formato OpenType Fuente Compacto (CFF) El controlador podría permitir la elevación de privilegios  MS10-069: Vulnerabilidad en Windows Client/Server Runtime Subsystem podría permitir elevación de privilegios (2121546)  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)  MS11-056 Vulnerabilidad en el subsistema cliente/servidor en tiempo de ejecución podría permitir la elevación de privilegios.  MS11-074: Vulnerabilidad en Microsoft SharePoint podría permitir elevación de privilegios (2451858)  MS12-003: Vulnerabilidad en el Subsistema de Windows Client/Server Run-time podría permitir elevación de privilegios (2646524)  MS12-006: Vulnerabilidad en SSL/TLS podría permitir revelación de información sensible (2643584)  MS12-018: 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)  MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.24.81 |

|  |  |  |
| --- | --- | --- |
| **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)  MS12-049: Vulnerabilidad en TLS Could podría revelar informaciín sensible (2655992)  MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualizaciones de Seguridad**

|  |
| --- |
| **IP** |
| 99.40.24.86 |

|  |  |  |
| --- | --- | --- |
| **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 KB2641690: Certificados Digitales Fraudulentos podrÃ­an permitir Spoofing  MS KB2718704: Certificados Digitales podrían permitir 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)  MS10-070: Vulnerabilidad en ASP.NET podría permitir la revelación de información (2418042)  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)  MS11-074: Vulnerabilidad en Microsoft SharePoint podría permitir elevación de privilegios (2451858)  MS12-003: Vulnerabilidad en el Subsistema de Windows Client/Server Run-time podría permitir elevación de privilegios (2646524)  MS12-006: Vulnerabilidad en SSL/TLS podría permitir revelación de información sensible (2643584)  MS12-018: 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)  MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517) | | |
| 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. | | |