**Segmento 99.41.16.0**

**Falta de Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.105 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Alta** |
| CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) |
| **Lista de Actualizaciones:** | | |
|  | | |
| MS10-012: Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código  MS11-028: Vulnerabilidad en .NET Framework, podría permitir la ejecución de código arbitrario  MS11-039: Vulnerabilidad en .NET y Microsoft Silverlight podría permitir ejecución remota de código (2514842)  MS11-044: Vulnerabilidad en .NET Framework podría permitir ejecución de código remota (2538814)  MS11-078: Vulnerabilidad en .NET Framework y Microsoft Silverlight podría permitir ejecución remota de código (2604930)  MS11-100: Vulnerabilidad en .NET Framework podría permitir elevación de privilegios (2638420)  MS12-016: Vulnerabilidad en .NET Framework y Microsoft Silverlight podrían permitir ejecución de código remoto (2651026)  MS12-025: Vulnerabilidad en .NET Framework podría ocasionar ejecución remota de código (2671605)  MS12-035: Vulnerabilidad en .NET Framework podría permitir ejecución remota de código (2693777)  MS12-038: Vulnerabilidad en .NET Framework podría permitir ejecución de código remoto (2706726)  MS12-074: Vulnerabilidad en .NET Framework podría permitir la ejecución de código remoto (2745030)  MS13-004: Vulnerabilidad en .NET Framework podría permitir la elevación de privilegios (2769324)  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)  MS13-046: Vulnerabilidad en Windows Kernel-Mode Driver podría Actualización de Seguridad Acumulativa para Internet Explorer permitir la elevación de privilegios (2840221) | | |
| 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 Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.106 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Alta** |
| CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) |
| **Lista de Actualizaciones:** | | |
|  | | |
| MS10-012: Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código  MS11-028: Vulnerabilidad en .NET Framework, podría permitir la ejecución de código arbitrario  MS11-039: Vulnerabilidad en .NET y Microsoft Silverlight podría permitir ejecución remota de código (2514842)  MS11-044: Vulnerabilidad en .NET Framework podría permitir ejecución de código remota (2538814)  MS11-078: Vulnerabilidad en .NET Framework y Microsoft Silverlight podría permitir ejecución remota de código (2604930)  MS11-100: Vulnerabilidad en .NET Framework podría permitir elevación de privilegios (2638420)  MS12-016: Vulnerabilidad en .NET Framework y Microsoft Silverlight podrían permitir ejecución de código remoto (2651026)  MS12-025: Vulnerabilidad en .NET Framework podría ocasionar ejecución remota de código (2671605)  MS12-035: Vulnerabilidad en .NET Framework podría permitir ejecución remota de código (2693777)  MS12-038: Vulnerabilidad en .NET Framework podría permitir ejecución de código remoto (2706726)  MS12-074: Vulnerabilidad en .NET Framework podría permitir la ejecución de código remoto (2745030)  MS13-004: Vulnerabilidad en .NET Framework podría permitir la elevación de privilegios (2769324)  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)  MS13-046: Vulnerabilidad en Windows Kernel-Mode Driver podría Actualización de Seguridad Acumulativa para Internet Explorer permitir la elevación de privilegios (2840221) | | |
| 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 Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.112 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Alta** |
| CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) |
| **Lista de Actualizaciones:** | | |
|  | | |
| MS KB2269637: Carga insegura de librerías podría permitir ejecución remota de código  MS12-027: Vulnerabilidad en Windows Common Controls podría ocasionar ejecución de código remoto (2664258)  MS12-060: Vulnerabilidad en Windows Common Controls podría permitir la ejecución de código remoto (2720573)  MS12-072: Vulnerabilidad en Windows Shell podría permitir la ejecución de código remoto (2727528)  "MS12-074: Vulnerabilidad en .NET Framework podría permitir la ejecución de código remoto (2745030)  "  MS12-075: Vulnerabilidad en drivers del kernel de Windows podrían permitir la ejecución de código remoto(2761226)  MS12-077: Actualización de Seguridad para Internet Explorer (2761465)  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  MS12-082: Vulnerabilidad en DirectPlay podría permitir la ejecución de código remoto (2770660)  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)  MS13-008: 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)  MS13-021: 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)  MS13-031: Vulnerabilidad en el kernel de Windows podría permitir la elevación de privilegios (2813170)  MS13-033: Vulnerabilidad en Windows Client/Server Run-time Subsystem podría permitir la escalación de privilegios(2820917)  MS13-036: Vulnerabilidad en el Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2829996)  MS13-046: Vulnerabilidad en Windows Kernel-Mode Driver podría Actualización de Seguridad Acumulativa para Internet Explorer permitir la elevación de privilegios (2840221) | | |
| 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 Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.113 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Alta** |
| CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) |
| **Lista de Actualizaciones:** | | |
|  | | |
| MS KB2269637: Carga insegura de librerías podría permitir ejecución remota de código  MS10-012: Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código  MS12-072: Vulnerabilidad en Windows Shell podría permitir la ejecución de código remoto (2727528)  "MS12-074: Vulnerabilidad en .NET Framework podría permitir la ejecución de código remoto (2745030)  "  MS12-075: Vulnerabilidad en drivers del kernel de Windows podrían permitir la ejecución de código remoto(2761226)  MS12-077: Actualización de Seguridad para Internet Explorer (2761465)  MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534)  MS12-081: Vulnerabilidad en Windows en el componente de manejo de archivos podría permitir la ejecución de código remoto (2758857)  MS12-082: Vulnerabilidad en DirectPlay podría permitir la ejecución de código remoto (2770660)  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)  MS13-008: 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)  MS13-021: 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)  MS13-031: Vulnerabilidad en el kernel de Windows podría permitir la elevación de privilegios (2813170)  MS13-033: Vulnerabilidad en Windows Client/Server Run-time Subsystem podría permitir la escalación de privilegios(2820917)  MS13-036: Vulnerabilidad en el Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2829996)  MS13-046: Vulnerabilidad en Windows Kernel-Mode Driver podría Actualización de Seguridad Acumulativa para Internet Explorer permitir la elevación de privilegios (2840221) | | |
| 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 Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.115 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Alta** |
| CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) |
| **Lista de Actualizaciones:** | | |
|  | | |
| MS KB2269637: Carga insegura de librerías podría permitir 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 Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.122 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Alta** |
| CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) |
| **Lista de Actualizaciones:** | | |
|  | | |
| MS10-012: Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código  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 Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.154 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Alta** |
| CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) |
| **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 Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.164 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Alta** |
| CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) |
| **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 Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.183 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Alta** |
| CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) |
| **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)  MS11-090: 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 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)  MS13-021: 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)  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)  MS13-041: Vulnerabilidad en Lync podría permitir la ejecución de código remoto (2834695)  MS13-046: Vulnerabilidad en Windows Kernel-Mode Driver podría Actualización de Seguridad Acumulativa para Internet Explorer permitir la elevación de privilegios (2840221) | | |
| 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 Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.197 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Alta** |
| CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) |
| **Lista de Actualizaciones:** | | |
|  | | |
| MS 2695962: Actualización para ActiveX en sus Kill Bits (2695962)  MS KB2506014: Update for the Windows Operating System Loader  MS KB2719662: Vulnerabilidades en Gadgets podría permitir la ejecución de código remoto  MS10-012: Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código  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  MS11-032: 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)  MS11-048: 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.  MS11-072: 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)  MS11-076: Vulnerabilidad en Windows Media Center podría permitir la ejecución remota (2604926)  MS11-089: Una vulnerabilidad en Microsoft Office podría permitir la ejecución remota de código  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 ejecución cliente / servidor podría permitir la elevación de privilegios  MS12-015: Vulnerabilidades en Microsoft Visio Viewer 2010 podrían permitir ejecución remota de código (2663510)  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)  MS12-031: Vulnerabilidad en Microsoft Visio Viewer 2010 podría ocasionar ejecución remota de código (2597981)  MS12-046: Vulnerabilidad en Visual Basic for Applications podría permitir la ejecución de código remoto (2707960)  MS12-052: Actualizaciones de seguridad acumulativas para Internet Explorer (2722913)  MS12-057: Microsoft Office permite la ejecución de código remoto (2731879)  MS12-059: Microsoft Visio y Visio Viewer permite la ejecución de código remoto (2733918)  MS12-063: Actualización acumulativa de seguridad para Internet Explorer (2744842)  MS12-064: Vulnerabilidad en Microsoft Word podría permitir la ejecución de código remoto (2742319)  "MS12-074: Vulnerabilidad en .NET Framework podría permitir la ejecución de código remoto (2745030)  "  MS12-076: Vulnerabilidad en Microsoft Office podría permitir la ejecución de código remoto (2720184)  MS12-077: Actualización de Seguridad para Internet Explorer (2761465)  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)  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)  MS13-004: 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)  MS13-022: Vulnerabilidad en Microsoft Silverlight podría permitir ejecución de código remoto (2814124)  MS13-023: Vulnerabilidad en Microsoft Visio Viewer 2010 podría permitir la ejecución de código remoto (2801261)  MS13-025: Vulnerabilidad en Microsoft OneNote podría permitir la divulgación de información sensible(2816264)  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)  MS13-041: Vulnerabilidad en Lync podría permitir la ejecución de código remoto (2834695)  MS13-046: Vulnerabilidad en Windows Kernel-Mode Driver podría Actualización de Seguridad Acumulativa para Internet Explorer permitir la elevación de privilegios (2840221) | | |
| 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 Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.203 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Alta** |
| CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) |
| **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 Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.212 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Alta** |
| CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) |
| **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 Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.219 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Alta** |
| CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) |
| **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 Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.22 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Alta** |
| CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) |
| **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: 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.  MS11-027: 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  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)  MS13-036: Vulnerabilidad en el Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2829996)  MS13-041: Vulnerabilidad en Lync podría permitir la ejecución de código remoto (2834695)  MS13-046: Vulnerabilidad en Windows Kernel-Mode Driver podría Actualización de Seguridad Acumulativa para Internet Explorer permitir la elevación de privilegios (2840221) | | |
| 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 Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.220 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Alta** |
| CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) |
| **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 Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.224 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Alta** |
| CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) |
| **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 Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.242 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Alta** |
| CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) |
| **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 Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.248 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Alta** |
| CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) |
| **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 Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.252 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Alta** |
| CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) |
| **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 Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.105 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Media** |
| Medio / CVSS Base Score : 6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) |
| **Lista de Actualizaciones:** | | |
|  | | |
| MS11-047: Vulnerabilidad en Hyper-V podría permitir Denegación de Servicio (2525835)  MS11-069: Vulnerabilidad en NET Framework podría permitir la divulgación de información (2.567.951)  MS13-007: Vulnerabilidad en Open Data Protocol podría permitir una denegación de servicio (2769327)  MS13-018: Vulnerabilidad en TCP/IP que podría permitir causar una denegación de servicio (2790655)  MS13-037: Actualización de Seguridad Acumulativa para Internet Explorer (2829530)  MS13-038: Actualización de Seguridad Acumulativa para Internet Explorer (2847204)  MS13-040: Vulnerabilidad en .NET Framework podría permitir la suplantación de identidad (2836440) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.106 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Media** |
| Medio / CVSS Base Score : 6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) |
| **Lista de Actualizaciones:** | | |
|  | | |
| MS11-047: Vulnerabilidad en Hyper-V podría permitir Denegación de Servicio (2525835)  MS11-069: Vulnerabilidad en NET Framework podría permitir la divulgación de información (2.567.951)  MS13-007: Vulnerabilidad en Open Data Protocol podría permitir una denegación de servicio (2769327)  MS13-018: Vulnerabilidad en TCP/IP que podría permitir causar una denegación de servicio (2790655)  MS13-037: Actualización de Seguridad Acumulativa para Internet Explorer (2829530)  MS13-038: Actualización de Seguridad Acumulativa para Internet Explorer (2847204)  MS13-040: Vulnerabilidad en .NET Framework podría permitir la suplantación de identidad (2836440) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.112 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Media** |
| Medio / CVSS Base Score : 6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) |
| **Lista de Actualizaciones:** | | |
|  | | |
| Microsoft Windows Autenticación Nula en SMB  MS KB982316: elevación de privilegios a través de evadir Windows Service Isolation  MS11-049: Una vulnerabilidad en el Editor XML de Microsoft podría permitir la divulgación de información (2.543.893)  MS13-037: Actualización de Seguridad Acumulativa para Internet Explorer (2829530)  MS13-040: Vulnerabilidad en .NET Framework podría permitir la suplantación de identidad (2836440) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.113 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Media** |
| Medio / CVSS Base Score : 6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) |
| **Lista de Actualizaciones:** | | |
|  | | |
| Microsoft Windows Autenticación Nula en SMB  MS KB982316: elevación de privilegios a través de evadir Windows Service Isolation  MS13-037: Actualización de Seguridad Acumulativa para Internet Explorer (2829530)  MS13-038: Actualización de Seguridad Acumulativa para Internet Explorer (2847204)  MS13-040: Vulnerabilidad en .NET Framework podría permitir la suplantación de identidad (2836440)  Terminal Services Vulnerable a Man in The Midle (Ataque de hombre en medio) | | |
| 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 Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.115 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Media** |
| Medio / CVSS Base Score : 6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) |
| **Lista de Actualizaciones:** | | |
|  | | |
| Microsoft Windows Autenticación Nula en SMB  MS KB982316: elevación de privilegios a través de evadir Windows Service Isolation  Terminal Services Vulnerable a Man in The Midle (Ataque de hombre en medio) | | |
| 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 Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.183 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Media** |
| Medio / CVSS Base Score : 6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) |
| **Lista de Actualizaciones:** | | |
|  | | |
| MS 2647518: Actualización para ActiveX Kill Bits (2647518)  MS KB2728973: Certificados digitales no autorizados podrían permitir la suplantación de identidad  MS11-009: Vulnerabilidad los motores de scripting de JScript y VBScript podrían permitir la divulgación de información  MS11-026: Vulnerabilidad en MHTML podría permitir la divulgación de información  MS11-037: Múltiples Vulnerabilidades en MHTML podrían permitir revelación de información (2544893)  MS11-066: Una vulnerabilidad en el control Microsoft Chart podría permitir la divulgación de información  MS13-006: Vulnerabilidad en Microsoft Windows podría permitir la evasión de restricciones de seguridad (2785220)  MS13-007: Vulnerabilidad en Open Data Protocol podría permitir una denegación de servicio (2769327)  MS13-037: Actualización de Seguridad Acumulativa para Internet Explorer (2829530)  MS13-038: Actualización de Seguridad Acumulativa para Internet Explorer (2847204)  MS13-040: Vulnerabilidad en .NET Framework podría permitir la suplantación de identidad (2836440) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.197 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Media** |
| Medio / CVSS Base Score : 6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) |
| **Lista de Actualizaciones:** | | |
|  | | |
| MS 2647518: Actualización para ActiveX Kill Bits (2647518)  MS11-026: Vulnerabilidad en MHTML podría permitir la divulgación de información  MS11-037: Múltiples Vulnerabilidades en MHTML podrían permitir revelación de información (2544893)  MS11-074: Vulnerabilidad en Microsoft SharePoint podría permitir elevación de privilegios (2451858)  MS12-050: Vulnerabilidades en SharePoint podrían permitir la elevación de privilegios (2695502)  MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517)  MS13-006: Vulnerabilidad en Microsoft Windows podría permitir la evasión de restricciones de seguridad (2785220)  MS13-007: Vulnerabilidad en Open Data Protocol podría permitir una denegación de servicio (2769327)  MS13-018: Vulnerabilidad en TCP/IP que podría permitir causar una denegación de servicio (2790655)  MS13-035: Vulnerabilidad en HTML Sanitization Component podría permitir la elevación de privilegios (2821818)  MS13-037: Actualización de Seguridad Acumulativa para Internet Explorer (2829530)  MS13-038: Actualización de Seguridad Acumulativa para Internet Explorer (2847204)  MS13-040: Vulnerabilidad en .NET Framework podría permitir la suplantación de identidad (2836440) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.22 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Media** |
| Medio / CVSS Base Score : 6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) |
| **Lista de Actualizaciones:** | | |
|  | | |
| MS 2647518: Actualización para ActiveX Kill Bits (2647518)  MS KB2728973: Certificados digitales no autorizados podrían permitir la suplantación de identidad  MS11-009: Vulnerabilidad los motores de scripting de JScript y VBScript podrían permitir la divulgación de información  MS11-026: Vulnerabilidad en MHTML podría permitir la divulgación de información  MS11-037: Múltiples Vulnerabilidades en MHTML podrían permitir revelación de información (2544893)  MS11-066: Una vulnerabilidad en el control Microsoft Chart podría permitir la divulgación de información  MS13-006: Vulnerabilidad en Microsoft Windows podría permitir la evasión de restricciones de seguridad (2785220)  MS13-007: Vulnerabilidad en Open Data Protocol podría permitir una denegación de servicio (2769327)  MS13-037: Actualización de Seguridad Acumulativa para Internet Explorer (2829530)  MS13-038: Actualización de Seguridad Acumulativa para Internet Explorer (2847204)  MS13-040: Vulnerabilidad en .NET Framework podría permitir la suplantación de identidad (2836440) | | |
| Solución: | | |
| Realizar las actualizaciones de seguridad correspondientes provistas por Microsoft, recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Falta de Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.74 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Media** |
| Medio / CVSS Base Score : 6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N) |
| **Lista de Actualizaciones:** | | |
|  | | |
| Terminal Services Vulnerable a Man in The Midle (Ataque de hombre en medio) | | |
| 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 Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.113 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Baja** |
| Baja / CVSS Base Score : 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N) |
| **Lista de Actualizaciones:** | | |
|  | | |
| El servicio de Terminal Services no es FIPS-140 compliant. | | |
| 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 Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.115 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Baja** |
| Baja / CVSS Base Score : 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N) |
| **Lista de Actualizaciones:** | | |
|  | | |
| El servicio de Terminal Services no es FIPS-140 compliant. | | |
| 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 Actualización de Seguridad**

|  |
| --- |
| **IP** |
| 99.41.16.74 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** |  | 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. |
| **Baja** |
| Baja / CVSS Base Score : 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N) |
| **Lista de Actualizaciones:** | | |
|  | | |
| El servicio de Terminal Services no es FIPS-140 compliant. | | |
| 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. | | |