A continuación se proporciona la lista de Actualizaciones de seguridad faltantes de acuerdo al fabricante.

## Segmento 99.41.16.0

**Actualizaciónes de criticidad Alta**

|  |  |
| --- | --- |
| Vulnerabilidad | Criticidad |
| MS 2695962: Actualización para ActiveX en sus Kill Bits (2695962) | Alta |
| MS KB2269637: Carga insegura de librerías podría permitir ejecución remota de código | Alta |
| MS KB2506014: Update for the Windows Operating System Loader | Alta |
| MS KB2719662: Vulnerabilidades en Gadgets podría permitir la ejecución de código remoto | Alta |
| MS08-069: Ejecución remota de código sobre Microsoft XML CoreServices (955218) | Alta |
| MS10-012: Vulnerabilidades en el servidor SMB podrían permitir la ejecución remota de código | Alta |
| MS11-007: Vulnerabilidad en el controlador del OpenType Compact Font Format (CFF) podría permitir la ejecución remota de código | Alta |
| MS11-015: Vulnerabilidades en Windows Media podrían permitir la ejecución remota de código | Alta |
| MS11-019: Vulnerabilidades en SMB Client permiten la ejecución de código remoto. | Alta |
| MS11-020: SMB presenta fallas en su implementación que permite la ejecución de código remoto | Alta |
| MS11-020: Vulnerabilidad en SMB server podría resultar en ejecución remota de código (2508429) | Alta |
| MS11-024: Vulnerabilidad en el editor Windows Fax Cover Page permite la ejecución de código remoto. | Alta |
| MS11-027: Actualización de seguridad acumulativa para ActiveX | Alta |
| MS11-028: Vulnerabilidad en .NET Framework, podría permitir la ejecución de código arbitrario | Alta |
| MS11-030: Vulnerabilidad en la resolución DNS podría permitir la ejecución remota de código | Alta |
| MS11-031: Vulnerabilidad en los motores de scripting de JScript y VBScript podría permitir la ejecución remota de código. | Alta |
| MS11-032: Vulnerabilidad en el controlador OpenType Compact Font Format (CFF) podría permitir la ejecución remota de código. | Alta |
| MS11-038: Vulnerabilidades en OLE Automation podrían permitir ejecución de código remoto (2476490) | Alta |
| MS11-039: Vulnerabilidad en .NET y Microsoft Silverlight podría permitir ejecución remota de código (2514842) | Alta |
| MS11-043: Una vulnerabilidad en el cliente SMB podrían permitir la ejecución remota de código (2536276) | Alta |
| MS11-044: Vulnerabilidad en .NET Framework podría permitir ejecución de código remota (2538814) | Alta |
| MS11-046: Vulnerabilidad en AncillaryFunction Driver podría permitir ejecución de código remota (2503665) | Alta |
| MS11-048: Vulnerabilidad en SMB Server podría ocasionar una denegación de servicio (2536275) | Alta |
| MS11-059: Una vulnerabilidad en el componente Microsoft Data Access podría permitir la ejecución remota de código (2560656) | Alta |
| MS11-071 Vulnerabilidad en componentes de Windows podría permitir ejecución de código de manera remota. | Alta |
| MS11-075: Vulnerabilidad en Microsoft Active Accessibility podría permitir la ejecución remota de código (2623699) | Alta |
| MS11-076: Vulnerabilidad en Windows Media Center podría permitir la ejecución remota (2604926) | Alta |
| MS11-078: Vulnerabilidad en .NET Framework y Microsoft Silverlight podría permitir ejecución remota de código (2604930) | Alta |
| MS11-090: ActualizaciÃ³n de seguridad para ActiveX | Alta |
| MS11-092: Una vulnerabilidad en Windows Media podría permitir la ejecución remota de código | Alta |
| MS11-097: Una vulnerabilidad en el subsistema de Windows en tiempo de ejecuciÃ³n cliente / servidor podrÃ­a permitir la elevaciÃ³n de privilegios | Alta |
| MS11-100: Vulnerabilidad en .NET Framework podría permitir elevación de privilegios (2638420) | Alta |
| MS12-016: Vulnerabilidad en .NET Framework y Microsoft Silverlight podrían permitir ejecución de código remoto (2651026) | Alta |
| MS12-025: Vulnerabilidad en .NET Framework podría ocasionar ejecución remota de código (2671605) | Alta |
| MS12-027: Vulnerabilidad en Windows CommonControls podría ocasionar ejecución de código remoto (2664258) | Alta |
| MS12-035: Vulnerabilidad en .NET Framework podría permitir ejecución remota de código (2693777) | Alta |
| MS12-038: Vulnerabilidad en .NET Framework podría permitir ejecución ed código remoto (2706726) | Alta |
| MS12-039: Vulnerabilidad en Lync podría permitir la ejecución de código remoto (2707956) | Alta |
| MS12-046: Vulnerabilidad en Visual Basic forApplications podría permitir la ejecución de código remoto (2707960) | Alta |
| MS12-052: Actualizaciones de seguridad acumulativas para Internet Explorer (2722913) | Alta |
| MS12-060: Vulnerabilidad en Windows CommonControls podría permitir la ejecución de código remoto (2720573) | Alta |
| MS12-063: Actualización acumulativa de seguridad para Internet Explorer (2744842) | Alta |
| MS12-072: Vulnerabilidad en Windows Shell podría permitir la ejecución de código remoto (2727528) | Alta |
| MS12-074: Vulnerabilidad en .NET Framework podría permitir la ejecución de código remoto (2745030) | Alta |
| MS12-075: Vulnerabilidad en drivers del kernel de Windows podrían permitir la ejecución de código remoto(2761226) | Alta |
| MS12-077: Actualización de Seguridad para Internet Explorer (2761465) | Alta |
| MS12-078: Vulnerabilidad en el Kernel-Mode Drivers podrían permitir ejecución remota de código (2783534) | Alta |
| MS12-081: Vulnerabilidad en Windows en el componente de manejo de archivos podría permitir la ejecución de código remoto (2758857) | Alta |
| MS12-082: Vulnerabilidad en DirectPlay podría permitir la ejecución de código remoto (2770660) | Alta |
| MS13-001: Vulnerabilidad en Windows PrintSpoolerComponents podría permitir la ejecución remota de código (2769369) | Alta |
| MS13-002: Vulnerabilidad en Microsoft XML podría permitir la ejecución de código remoto (2756145) | Alta |
| MS13-004: Vulnerabilidad en .NET Framework podría permitir la elevación de privilegios (2769324) | Alta |
| MS13-005: Vulnerabilidad en Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2778930) | Alta |
| MS13-008: Actualización de seguridad acumulativa para Internet Explorer (2799329) | Alta |
| MS13-009: Actualización de seguridad para Internet Explorer (2792100) | Alta |
| MS13-010: Vulnerabilidad en Vector MarkupLanguage (VML) que podría permitir la ejecución remota de código (2797052) | Alta |
| MS13-011: Vulnerabilidad en Media Decompression que podría permitir la ejecución remota de código (2780091) | Alta |
| MS13-015: Vulnerabilidad en .NET Framework que podría permitir la elevación de privilegios (2800277) | Alta |
| MS13-016: Vulnerabilidades en Windows Kernel-Mode Driver que podrían permitir la elevación de privilegios (2778344) | Alta |
| MS13-017: Vulnerabilidades en Windows Kernel que podrían permitir la elevación de privilegios (2799494) | Alta |
| MS13-019: Vulnerabilidad en Windows Client/Server Run-time Subsystem (CSRSS) que puede permitir la elevación de privilegios (2790113) | Alta |
| MS13-021: Actualizaciones de seguridad para Internet Explorer (2809289) | Alta |
| MS13-022: Vulnerabilidad en Microsoft Silverlight podría permitir ejecución de código remoto (2814124) | Alta |
| MS13-027: Vulnerabilidad en Kernel-Mode Drivers podría permitir elevación de privilegios de seguridad (2807986) | Alta |
| MS13-028: Actualización de seguridad para Internet Explorer (2817183) | Alta |
| MS13-029: Vulnerabilidad en Remote Desktop Client podría permitir la ejecución remota de código (2828223) | Alta |
| MS13-031: Vulnerabilidad en el kernel de Windows podría permitir la elevación de privilegios (2813170) | Alta |
| MS13-033: Vulnerabilidad en Windows Client/Server Run-time Subsystem podría permitir la escalación de privilegios(2820917) | Alta |
| MS13-036: Vulnerabilidad en el Windows Kernel-Mode Driver podría permitir la elevación de privilegios (2829996) | Alta |
| MS13-041: Vulnerabilidad en Lync podría permitir la ejecución de código remoto (2834695) | Alta |
| MS13-046: Vulnerabilidad en Windows Kernel-Mode Driver podría Actualización de Seguridad Acumulativa para Internet Explorer ermitir la elevación de privilegios (2840221) | Alta |

**Actualizaciónes de criticidad Media**

|  |  |
| --- | --- |
| Vulnerabilidad | Criticidad |
| MS 2647518: Actualización para ActiveX Kill Bits (2647518) | Media |
| MS KB2728973: Certificados digitales no autorizados podrían permitir la suplantación de identidad | Media |
| MS KB982316: elevación de privilegios a través de evadir Windows ServiceIsolation | Media |
| MS11-009: Vulnerabilidad los motores de scripting de JScript y VBScript podrían permitir la divulgación de información | Media |
| MS11-026: Vulnerabilidad en MHTML podría permitir la divulgación de información | Media |
| MS11-037: Múltiples Vulnerabilidades en MHTML podrían permitir revelación de información (2544893) | Media |
| MS11-047: Vulnerabilidad en Hyper-V podría permitir Denegación de Servicio (2525835) | Media |
| MS11-049: Una vulnerabilidad en el Editor XML de Microsoft podría permitir la divulgación de información (2.543.893) | Media |
| MS11-066: Una vulnerabilidad en el control Microsoft Chart podría permitir la divulgación de información | Media |
| MS11-069: Vulnerabilidad en NET Framework podría permitir la divulgación de información (2.567.951) | Media |
| MS12-066: Vulnerabilidad en la sanitización de HTML podría permitir la elevación de privilegios (2741517) | Media |
| MS13-006: Vulnerabilidad en Microsoft Windows podría permitir la evasión de restricciones de seguridad (2785220) | Media |
| MS13-007: Vulnerabilidad en Open Data Protocol podría permitir una denegación de servicio (2769327) | Media |
| MS13-018: Vulnerabilidad en TCP/IP que podría permitir causar una denegación de servicio (2790655) | Media |
| MS13-035: Vulnerabilidad en HTML SanitizationComponent podría permitir la elevación de privilegios (2821818) | Media |
| MS13-037: Actualización de Seguridad Acumulativa para Internet Explorer (2829530) | Media |
| MS13-038: Actualización de Seguridad Acumulativa para Internet Explorer (2847204) | Media |
| MS13-040: Vulnerabilidad en .NET Framework podría permitir la suplantación de identidad (2836440) | Media |

***Microsoft Office***

|  |  |
| --- | --- |
| Vulnerabilidad | Criticidad |
| MS11-072: Vulnerabilidades en Microsoft Excel podría permitir la ejecución remota de código (2587505) | Alta |
| MS11-089: Una vulnerabilidad en Microsoft Office podría permitir la ejecución remota de código | Alta |
| MS12-030: Vulnerabilidad en Microsoft Office podría ocasionar ejecución remota de código (2663830) | Alta |
| MS12-031: Vulnerabilidad en Microsoft Visio Viewer 2010 podría ocasionar ejecución remota de código (2597981) | Alta |
| MS12-057: Microsoft Office permite la ejecución de código remoto (2731879) | Alta |
| MS12-059: Microsoft Visio y Visio Viewer permite la ejecución de código remoto (2733918) | Alta |
| MS12-064: Vulnerabilidad en Microsoft Word podría permitir la ejecución de código remoto (2742319) | Alta |
| MS12-076: Vulnerabilidad en Microsoft Office podría permitir la ejecución de código remoto (2720184) | Alta |
| MS12-079: Vulnerabili en Microsoft Word podría permitir la ejecución remota de código (2780642) | Alta |
| MS13-023: Vulnerabilidad en Microsoft Visio Viewer 2010 podría permitir la ejcución de código remoto (2801261) | Alta |
| MS13-025: Vulnerabilidad en Microsoft OneNote podría permitir la divulgación de información sensible(2816264) | Alta |
| MS12-015: Vulnerabilidades en Microsoft Visio Viewer 2010 podrían permitir ejecución remota de código (2663510) | Alta |

|  |  |
| --- | --- |
| Vulnerabilidad | Criticidad |
| MS11-074: Vulnerabilidad en Microsoft SharePoint podría permitir elevación de privilegios (2451858) | Media |
| MS12-050: Vulnerabilidades en SharePoint podrían permitir la elevación de privilegios (2695502) | Media |

***Otras Aplicaciones***

**Actualizaciónes de criticidad Alta**

|  |  |
| --- | --- |
| Vulnerabilidad | Criticidad |
| Acceso a recursos compartidos | Alta |
| ActiveX Conjunto de actualizaciones | Alta |
| ActiveX Controles Data Dynamics ActiveBar permiten la ejecución de código | Alta |
| Adobe Flash Player <= 10.3.183.7 Múltiples Vulnerabilidades (APSB11-26) | Alta |
| Adobe Flash Player Detección de versión no soportada | Alta |
| Oracle Java JDK / JRE 6 < Actualización para corregir múltiples vulnerabilidades | Alta |
| Oracle Java SE Múltiples Vulnerabilidades (June 2012 CPU) | Alta |

**Actualizaciónes de criticidad Media**

|  |  |
| --- | --- |
| Vulnerabilidad | Criticidad |
| Adobe Flash Player < 10.3.181.22 Cross-Site Scripting (XSS) (APSB11-13) | Media |
| Microsoft Windows Autenticación Nula en SMB | Media |
| Terminal Services Vulnerable a Man in TheMidle (Ataque de hombre en medio) | Media |