**ActiveX Conjunto de actualizaciones**

|  |
| --- |
| IP |
| 99.18.216.105 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alta / CVSS Base Score : 9.3  (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)  (CVSS2#E:F/RL:OF/RC:C) | Actualizar los controles ActiveX del host Windows remoto. Tenga en cuenta que los controles afectados son de otros fabricantes que han pedido a Microsoft a impedir que sus controles se ejecuten en Internet Explorer. |
| Solución: | | |
| Se recomienda actualizar los controles ActiveX. recordando que toda actualización puede tener impacto en los sistemas. Si la organización decide no instalar la actualización, esto debe de estar documentado.  Para más información, visite el siguiente enlace:  <http://support.microsoft.com/kb/2562937> | | |

**El agente de SNMP tiene configurada la comunidad "public"**

|  |
| --- |
| IP |
| 99.18.216.241 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **UDP/161** | **Alta**  Alta / CVSS Base Score : 9.3  (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)  (CVSS2#E:F/RL:OF/RC:C) | Es posible obtener el nombre de la comunidad por default: "public" esta configurada en el agente del protocolo SNMP. Un atacante remoto puede utilizar esta mala configuración para obtener información sensible del sistema afectado. |
| Solución: | | |
| Cambiar el nombre de la comunidad a una personalizada por el administrador del servicio, si es posible, configurar la versión 3 de SNMP, que incluye un mecanismo de cifrado para las respuestas del servicio.  Evaluar si el servicio no es necesario y en su defecto deshabilitarlo. | | |

**WinRAR < 3.71Vulnerabilidades en el Manejo de Archivos**

|  |
| --- |
| **IP** |
| 99.18.216.105 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Alta**  Alta / CVSS Base Score : 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C) | La versión de WinRAR en el sistema remoto es susceptible a diversos problemas de corrupción y desbordamientos de buffer (buffer overflow). Un atacante que engañe a un usuario con un archivo malicioso podría ejecutar código con los permisos del usuario activo. |
| Solución: | | |
| Actualizar a WinRAR 3.90 o superior.  http://www.winrar.es/  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe ser documentado. | | |

**Terminal Services Vulnerable a Man in The Midle (Ataque de hombre en medio)**

|  |  |  |
| --- | --- | --- |
| **IP** | | |
| 99.18.216.68 | 99.18.216.225 | 99.18.216.20 |
| 99.18.216.180 | 99.18.216.176 | 99.18.216.174 |
| 99.18.216.172 | 99.18.216.168 | 99.18.216.165 |
| 99.18.216.163 | 99.18.216.157 | 99.18.216.156 |
| 99.18.216.155 | 99.18.216.154 | 99.18.216.153 |
| 99.18.216.152 | 99.18.216.150 | 99.18.216.143 |
| 99.18.216.110 | 99.18.216.105 | 99.18.216.101 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/3389** | **Media**  Media / CVSS Base Score : 5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P) | El servicio Terminal Services en el host remoto es propenso a un ataque de hombre en medio y robo de sesión con lo cual un atacante podría obtener acceso al sistema con las credenciales del usuario conectado vía Terminal Service. |
| Solución: | | |
| Forzar el uso de SSL en las conexiones. Si no es posible crear un túnel de ssh para el uso del servicio. | | |

**Certificados Digitales Fraudulentos podrían permitir la suplantación de identidad**

|  |
| --- |
| **IP** |
| 99.18.216.105 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/3389** | **Media**  Media / CVSS Base Score : 5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P) | Debido a la emisiÃ³n de varios certificados SSL fraudulentos de la entidad emisora ââde certificados DigiNotar. Algunos de los certificados almacenados en el host remoto no son de confianza. |
| Solución: | | |
| Se recomienda quitar certificados emitidos por Diginotar del almacén de certificados.  Para más información, visite el siguiente enlace:  http://support.microsoft.com/kb/2616676 | | |

**Almacenamiento de credenciales en memoria**

|  |
| --- |
| **IP** |
| 99.18.216.176 |
| 99.18.216.105 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Baja**  Baja / CVSS Base Score : 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N) | La llave de registro \nHKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount\nis está establecida con un valor diferente a 0, esto significa que el sistema remoto almacena locamente las contraseñas en cache para permitir el acceso automático de los usuario en caso de una falla del PDC. |
| Solución: | | |
| Establecer el valor de la llave de registro a 0 | | |

**El servicio de Terminal Services no es FIPS-140 compliant.**

|  |  |  |
| --- | --- | --- |
| **IP** | | |
| 99.18.216.68 | 99.18.216.225 | 99.18.216.20 |
| 99.18.216.180 | 99.18.216.176 | 99.18.216.174 |
| 99.18.216.172 | 99.18.216.168 | 99.18.216.165 |
| 99.18.216.163 | 99.18.216.157 | 99.18.216.156 |
| 99.18.216.155 | 99.18.216.154 | 99.18.216.153 |
| 99.18.216.152 | 99.18.216.150 | 99.18.216.143 |
| 99.18.216.110 | 99.18.216.105 | 99.18.216.101 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/3389** | **Baja**  Baja / CVSS Base Score : 2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N) | El nivel de cifrado utilizado en el servicio de escritorio remoto no es FIPS-140 compliant. |
| Solución: | | |
| Establecer el nivel de cifrado del protocolo RDP a 4 "FIPS Compliant". | | |

**Servicio de Telnet**

|  |
| --- |
| **IP** |
| 99.18.216.241 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/23** | **Baja** | El sistema remoto está ejecutando el servicio telnet. Este servicio es usado para la administración remota de equipos. La arquitectura de este servicio, lo hace inseguro ya que la comunicación en el cliente y el servidor se lleva a cabo sin ningún cifrado, esto lo hace propenso a ataques de robo de sesión, el cual permite tomar control total del sistema. |
| Solución: | | |
| Validar el uso del servicio, en caso de no ser necesario, consultar al fabricante sobre la des habilitación del servicio, si es requerido entonces establecer un filtrado para la conexión al puerto/servicio. | | |