**Acceso a recursos compartidos**

|  |
| --- |
| IP |
| 10.113.2.98 |
| 10.113.2.97 |

|  |  |  |
| --- | --- | --- |
| **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) | Es posible acceder a los recursos compartidos vía SMB con las credenciales provistas. Dependiendo de los permisos, esto puede permitirá un atacante a leer/escribir información confidencial. |
| Solución: | | |
| Establecer permisos específicos de acceso, lectura y escritura para cada usuario que requiera utilizar los recursos. | | |

**Conficker Detección del Gusano**

|  |
| --- |
| IP |
| 10.113.2.97 |
| 10.113.2.93 |
| 10.113.2.92 |
| 10.113.2.100 |

|  |  |  |
| --- | --- | --- |
| **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) | El sistema remoto parece estar infectado por el gusano Conficker, este gusano permite a un atacante ejecutar código de manera arbitraria sobre el sistema vulnerable. Además el host infectado puede estar intentado propagar la infección en la red. |
| Solución: | | |
| Actualizar las firmas y motor de Antivirus y realizar un escaneo completo del sistema operativo. | | |

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

|  |
| --- |
| **IP** |
| 10.113.2.110 |

|  |  |  |
| --- | --- | --- |
| **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) | 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. | | |

**VMSA-2012-0009 : ESXi y ESX parches para solucionar problemas criticos de seguridad**

|  |
| --- |
| **IP** |
| 10.113.2.81 |
| 10.113.2.80 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Alta**  Alto / CVSS Base Score : 7.2  (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C) | El equipo remoto VMware ESX/ESXi se ve afectado de las siguientes vulnerabilidades:  - ESX NFS vulnerabilidad en el parseo de tráfico:  (CVE-2012-2448)  - VMware dispositivo de floppy problema de memoria (CVE-2012-2449)  - VMware SCSI problemas en los dispositivos de memoria (CVE-2012-2450) |
| Solución: | | |
| Aplicar los parches recomendados por el fabricante.  Recordando que toda actualización puede tener un impacto en los sistemas. Si la organización decide no instalar la actualización esto debe estar documentado. | | |

**Es posible acceder al sistema remoto con cuenta Guest en sistemas Microsoft Windows**

|  |
| --- |
| **IP** |
| 10.113.2.98 |
| 10.113.2.97 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/445** | **Media**  Media / CVSS Base Score : 4.3 (VSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N) | El sistema remoto cuenta con el sistema operativo Microsoft Windows, el cual permite acceder como guest (invitado), utilizando una cuenta aleatoria. |
| Solución: | | |
| En una group policy (politica de grupo) cambiar el valor de 'Network access: Sharing and security model for local accounts' de 'Guest only - local users authenticate as Guest' a 'Classic - local users authenticate as themselves'. | | |

**Microsoft Windows Autenticación Nula en SMB**

|  |  |  |  |
| --- | --- | --- | --- |
| **IP** | | | |
| 10.113.2.98 | 10.113.2.97 | 10.113.2.95 | 10.113.2.94 |
| 10.113.2.93 | 10.113.2.92 | 10.113.2.90 | 10.113.2.88 |
| 10.113.2.87 | 10.113.2.79 | 10.113.2.76 | 10.113.2.75 |
| 10.113.2.100 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/General** | **Media**  Media / CVSS Base Score : 5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N) | El equipo remoto permite acceder utilizando una sesión nula de SMB. Dependiendo de la configuración un atacante podría obtener información sobre el equipo remoto. |
| Solución: | | |
| Consultar las siguientes ligas para la solución  http://support.microsoft.com/kb/q143474/  http://support.microsoft.com/kb/q246261/ | | |

**SSL y SSH Protocolo de cifrado inseguro**

|  |
| --- |
| **IP** |
| 99.40.20.249 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/22**  **TCP/443** | **Media**  Media / CVSS Base Score : 5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P) | El servicio SSH en el sistema remoto acepta peticiones cifradas utilizando el protocolo SSH 1.33 y/o 1.5, el cual sufre de diversas deficiencias criptográficas y se encuentra en desuso. Un atacante podría aprovechar esto para realizar un ataque de hombre en medio. |
| Solución: | | |
| Deshabilitar el soporte para protocolo SSH 1.X y utilizar SSH 2.0 en su lugar. Configurar en el archivo de configuración httpd.conf o ssl.conf según corresponda, establecer.  SSLProtocol -ALL +SSLv3 +TLSv1  SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:-LOW:-SSLv2:-EXP | | |

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

|  |  |  |
| --- | --- | --- |
| **IP** | | |
| 10.113.2.99 | 10.113.2.98 | 10.113.2.97 |
| 10.113.2.96 | 10.113.2.95 | 10.113.2.94 |
| 10.113.2.93 | 10.113.2.92 | 10.113.2.91 |
| 10.113.2.90 | 10.113.2.88 | 10.113.2.87 |
| 10.113.2.79 | 10.113.2.76 | 10.113.2.75 |
| 10.113.2.69 | 10.113.2.100 |

|  |  |  |
| --- | --- | --- |
| **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. | | |

**Uso de llaves débiles para cifrado SSL**

|  |
| --- |
| **IP** |
| 10.113.2.110 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **TCP/443** | **Media**  Media / CVSS Base Score : 5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P) | El sistema remoto soporta el uso de llaves SSL débiles (<=56bits) que ofrecen un cifrado débil para la comunicación de los datos. |
| Solución: | | |
| Reconfigure el sistema afectado para evitar el uso de llaves débiles, se recomienda que las llaves sean de 128bits o superiores. | | |

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

|  |  |  |
| --- | --- | --- |
| **IP** | | |
| 10.113.2.99 | 10.113.2.98 | 10.113.2.97 |
| 10.113.2.96 | 10.113.2.95 | 10.113.2.94 |
| 10.113.2.93 | 10.113.2.92 | 10.113.2.91 |
| 10.113.2.90 | 10.113.2.88 | 10.113.2.87 |
| 10.113.2.79 | 10.113.2.76 | 10.113.2.75 |
| 10.113.2.69 | 10.113.2.100 |

|  |  |  |
| --- | --- | --- |
| **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 Telnet**

|  |
| --- |
| **IP** |
| 10.113.2.65 |

|  |  |  |
| --- | --- | --- |
| **Servicio** | **Impacto** | **Descripción de la vulnerabilidad** |
| **UDP/General** | **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. | | |