



FORMULARIO DE REVISIÓN TÉCNICA

1. FECHA Y HORA:

23/05/2024

2. APELLIDO Y NOMBRE DEL TÉCNICO A CARGO DE LA REVISIÓN:

Diego Castro

3. IDENTIFICACIÓN DEL DISPOSITIVO: (Marca, Modelo, Nro de Serie)

Device name DESKTOP-5SEERKP
Processor Intel(R) Core(TM) i7-4770 CPU @ 3.40GHz 3.40 GHz
Installed RAM 16,0 GB
Device ID xxx73DF7-B1CF-46B7-xxxx-42D9xxxxxxxx
Product ID 00XXX-XXXXX-00000-XX686
System type 64-bit operating system, x64-based processor

4. DIAGNÓSTICO INICIAL: (complete este ítem por cada evento de agresión que encuentre)

The screenshot displays the Avast Premium Security dashboard. At the top, there's a status bar with 'Avast Premium Security' on the left, a notification bell icon with '2' on the right, and a 'Menú' button. Below this, a progress bar shows four categories: 'Sistema operativo' (Problemas detectados), 'Virus y malware' (Todo correcto), 'Problemas avanzados' (Problemas detectados), and 'Problemas de rendimiento' (Problemas detectados). The main area lists several security alerts with icons and expandable details:

- Guardian de correo no protege actualmente ningún buzón en línea, pero puede proteger hasta 5**: Conecte su buzón en la nube a Guardián de correo para poder etiquetar como sospechosos correos electrónicos potencialmente peligrosos.
- Tiene protección contra ataques de explotación de vulnerabilidades de Protocolo de escritorio remoto**: Con Escudo de acceso remoto, usted decide qué direcciones IP pueden tener acceso remoto a su equipo.
- 8 documentos confidenciales desprotegidos**: Proteja sus datos privados, actualmente vulnerables al acceso no autorizado.
- Sitio web legítimo le está protegiendo de sitios web falsos**: Puede navegar y realizar compras y operaciones bancarias con mayor seguridad sabiendo que los sitios que visita son los reales.
- Puede borrar definitivamente 3 de sus archivos eliminados, para impedir que se restauren o usen de forma indebida**: El uso de Destructor de datos garantiza que los hackers no podrán restaurar ni usar indebidamente sus datos eliminados.
- Sandbox le permite navegar por internet o ejecutar aplicaciones en un entorno virtual seguro**: En un entorno completamente aislado del resto del sistema de su PC, Sandbox le permite ejecutar aplicaciones sospechosas sin correr riesgos.

At the bottom, there is a green 'RESOLVER TODO' button and a link to 'Omitir por ahora'.



a. **TIPO DE EVENTO: (Malware, Vulnerabilidad, Ataque)**
Vulnerabilidad

b. **IDENTIFIQUE EL COMPONENTE DE AGRESIÓN: (Nombre, versión, y demás características)**

Nombre: CVE-2020-9715

Versión: Afecta Adobe Acrobat Reader DC versiones anteriores a 2020.012.20048.

Características: Esta vulnerabilidad permite la escalación de privilegios a través de un manejo incorrecto de permisos de archivo.

c. **IDENTIFIQUE EL IMPACTO DE LAS AGRESIÓN: (Áreas o funcionalidades del equipo comprometidas, componentes infectados, etc)**

- Áreas comprometidas: Sistema operativo (Windows y macOS), acceso administrativo no autorizado.
- Componentes infectados: Archivos del sistema, permisos de usuario, configuraciones de seguridad.

d. **CAUSA PROBABLE: (Identifique la/s causa/s probables u origen de la agresión)**

- Origen: Apertura de un PDF malicioso enviado por correo electrónico o descargado de una fuente no confiable.

e. **SI ES UNA AMENAZA INTERNA, DESCRIBA LA SITUACIÓN OCURRIDA CON EL USUARIO:**

- Situación: El usuario abrió un documento PDF recibido de un remitente desconocido sin verificar su autenticidad, ejecutando así el código malicioso.

f. ACCIÓN DE CONTENCIÓN (y restauración a la situación inicial si corresponde):

- Contención:
 - g. Revocar los accesos no autorizados.
 - h. Actualizar Adobe Acrobat Reader a la versión más reciente.
 - i. Revisar y ajustar las políticas de permisos.
- Restauración:
 - j. Restablecer las configuraciones del sistema afectadas.
 - k. Verificar la integridad del sistema y restaurar archivos desde respaldos seguros.

I. HERRAMIENTAS UTILIZADAS:

- Antivirus: Norton Security, Bitdefender.

Nombre del estudiante: Diego Castro - **Fecha de elaboración:** 23/05/202

TALLER N°: 7

TEMA: ESCANEO DE VULNERABILIDADES Y A ANTIVIRUS EN UN PUESTO DE TRABAJO

Realice los siguientes controles sobre su computadora:

a - Si fue vulnerada la cámara web

No disponible.

b - Si tiene rastreadores

La búsqueda de rastreadores en el documento PDF proporcionado no arrojó resultados.

c - Si tiene algún malware

El documento PDF proporcionado afirma que Avast Premium Security detecta y bloquea amenazas de malware en tiempo real.

d - Si tiene algún virus

El documento PDF proporcionado afirma que Avast Premium Security detecta y bloquea amenazas de virus en tiempo real.

e - Si cuenta con puertos abiertos y a que redes está conectada

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell <https://aka.ms/powershell>

PS C:\Windows\system32> Get-NetTCPConnection

LocalAddress	LocalPort	RemoteAddress	RemotePort	State	AppliedSetting
::	49547	::	0	Bound	
::	49669	::	0	Listen	
::	49668	::	0	Listen	
::	49667	::	0	Listen	
::	49666	::	0	Listen	
::	49665	::	0	Listen	
::	49664	::	0	Listen	
:::1	27275	::	0	Listen	
:::1	12995	::	0	Listen	
:::1	12993	::	0	Listen	
:::1	12563	::	0	Listen	
:::1	12465	::	0	Listen	
:::1	12143	::	0	Listen	
:::1	12119	::	0	Listen	
:::1	12110	::	0	Listen	
:::1	12025	::	0	Listen	
::	7680	::	0	Listen	
::	445	::	0	Listen	
::	135	::	0	Listen	
0.0.0.0	65534	0.0.0.0	0	Bound	
0.0.0.0	65533	0.0.0.0	0	Bound	
0.0.0.0	65532	0.0.0.0	0	Bound	
0.0.0.0	65531	0.0.0.0	0	Bound	
0.0.0.0	65530	0.0.0.0	0	Bound	
0.0.0.0	65529	0.0.0.0	0	Bound	
0.0.0.0	65528	0.0.0.0	0	Bound	
0.0.0.0	65527	0.0.0.0	0	Bound	
0.0.0.0	65526	0.0.0.0	0	Bound	
0.0.0.0	65523	0.0.0.0	0	Bound	
0.0.0.0	65522	0.0.0.0	0	Bound	
0.0.0.0	65520	0.0.0.0	0	Bound	
0.0.0.0	65519	0.0.0.0	0	Bound	
0.0.0.0	65518	0.0.0.0	0	Bound	
0.0.0.0	65517	0.0.0.0	0	Bound	
0.0.0.0	65516	0.0.0.0	0	Bound	
0.0.0.0	65515	0.0.0.0	0	Bound	
0.0.0.0	65514	0.0.0.0	0	Bound	
0.0.0.0	65512	0.0.0.0	0	Bound	
0.0.0.0	65509	0.0.0.0	0	Bound	
0.0.0.0	65503	0.0.0.0	0	Bound	
0.0.0.0	65497	0.0.0.0	0	Bound	
0.0.0.0	65483	0.0.0.0	0	Bound	
0.0.0.0	65391	0.0.0.0	0	Bound	
0.0.0.0	65260	0.0.0.0	0	Bound	
0.0.0.0	65084	0.0.0.0	0	Bound	
0.0.0.0	64963	0.0.0.0	0	Bound	
0.0.0.0	64863	0.0.0.0	0	Bound	
0.0.0.0	64471	0.0.0.0	0	Bound	
0.0.0.0	63774	0.0.0.0	0	Bound	
0.0.0.0	63750	0.0.0.0	0	Bound	
0.0.0.0	62200	0.0.0.0	0	Bound	
0.0.0.0	62199	0.0.0.0	0	Bound	
0.0.0.0	61970	0.0.0.0	0	Bound	
0.0.0.0	61929	0.0.0.0	0	Bound	
0.0.0.0	61834	0.0.0.0	0	Bound	
0.0.0.0	61088	0.0.0.0	0	Bound	
0.0.0.0	60712	0.0.0.0	0	Bound	
0.0.0.0	60569	0.0.0.0	0	Bound	
0.0.0.0	60566	0.0.0.0	0	Bound	
0.0.0.0	60565	0.0.0.0	0	Bound	
0.0.0.0	60563	0.0.0.0	0	Bound	
0.0.0.0	60562	0.0.0.0	0	Bound	
0.0.0.0	60426	0.0.0.0	0	Bound	
0.0.0.0	60379	0.0.0.0	0	Bound	
0.0.0.0	60376	0.0.0.0	0	Bound	
0.0.0.0	60375	0.0.0.0	0	Bound	
0.0.0.0	60370	0.0.0.0	0	Bound	
0.0.0.0	60369	0.0.0.0	0	Bound	
0.0.0.0	60237	0.0.0.0	0	Bound	
0.0.0.0	59674	0.0.0.0	0	Bound	