PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Asociación de Bancos del Perú

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

272-2024-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aéreadel Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y lasempresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°272	Fecha: 25-11-2024 Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Los piratas informáticos aprovechan el controlador anti-rootkit de Avast para desactivar las protecciones		
Tipo de Ataque	Malware		Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Los investigadores de ciberseguridad de Trellix han identificado una campaña maliciosa que explota un controlador legítimo de Avast Anti-Rootkit, aswArPot.sys, para eludir la detección y tomar control del sistema objetivo al deshabilitar componentes de seguridad.

El abuso del controlador de Avast no es nuevo. En ataques previos, por ejemplo, en 2021, el ransomware Cuba utilizó un script que explotaba funciones del controlador anti-rootkit de Avast para desactivar defensas.

En 2022, investigadores de Trend Micro observaron el mismo controlador en un ataque del ransomware AvosLocker. En el mismo año, SentinelLabs reportó dos vulnerabilidades críticas (CVE-2022-26522 y CVE-2022-26523) presentes desde 2016, que permitían escalar privilegios para deshabilitar productos de seguridad. Avast solucionó estos problemas con actualizaciones silenciosas a finales de 2021.

2. DETALLES:

En una publicación de blog del 20 de noviembre, los investigadores de Trellix dijeron que, en lugar de usar un controlador especialmente diseñado para realizar sus actividades maliciosas, el malware utiliza un controlador de kernel confiable, lo que le da un aire de legitimidad, lo que le permite evitar generar alarmas mientras se prepara para socavar las defensas del sistema.

Este método se basa en la técnica de traer su propio controlador vulnerable (BYOVD), un enfoque que explota controladores legítimos con fallas de seguridad conocidas.

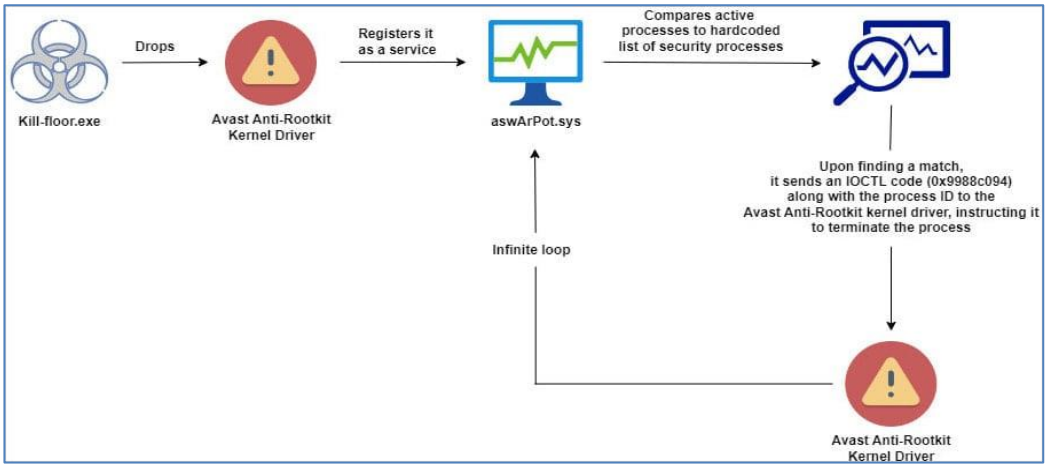
El malware involucrado, un AV Killer sin afiliación clara a una familia específica, cuenta con una lista codificada de 142 nombres de procesos de seguridad pertenecientes a diversos proveedores.

Security Process Names			
ERAAgent.exe	avpsus.exe	ekrn.exe	eguiProxy.exe
efwd.exe	avpui.exe	MsMpEng.exe	agentsvc.exe
SophosSafestore64.exe	mcupdatemgr.exe	QcShm.exe	ModuleCoreService.exe
PEFService.exe	McAWFwk.exe	mfeatp.exe	mfeesp.exe
mfefw.exe	mfewch.exe	mfehcs.exe	mfeensppl
mfemms.exe	mfevtps.exe	mcshield.exe	mfetp.exe
mfewc.exe	McCSPServiceHost.exe	Launch.exe	delegate.exe
McDiReg.exe	McPvTray.exe	McInstruTrack.exe	McUICnt.exe
ProtectedModuleHost.exe	MMSSHOST.exe	MfeAVSvc.exe	alsvc.exe
msmpeng.exe	sophosui.exe	avastsvc.exe	notifier.exe
ssdvagent.exe	avastui.exe	ntrtscan.exe	sspservice.exe
avp.exe	paui.exe	svcgenerichost.exe	pccntmon.exe
swc_service.exe	bcc.exe	psanhost.exe	swi_fc.exe
bccavsvc.exe	psuamain.exe	swi_service.exe	ccsvchst.exe
psuaservice.exe	tesvc.exe	clientmanager.exe	remediationservice.exe
TmCCSF.exe	coreframeworkhost.exe	repmgr.exe	tmcpmadapter.exe
coreserviceshell.exe	RepUtils.exe	tmlisten.exe	cpda.exe
repux.exe	updaterui.exe	cptraylogic.exe	savadminservice.exe
vapm.exe	cptrayui.exe	savapi.exe	VipreNis.exe
cylancesvc.exe	savservice.exe	vstskmgr.exe	ds_monitor.exe
avpsus.exe	SBAMSvc.exe	wrsa.exe	dsa.exe
sbamtray.exe	sophossafestore.exe	efrservice.exe	sbpimsvc.exe
sophoslivequeryservice.exe	epam_svc.exe	scanhost.exe	sophososquery.exe
epwd.exe	sdcservice.exe	sophosfimservice.exe	hmpalert.exe
sophosmtrextension.exe	hostedagent.exe	hostedagent.exe	sentinelagent.exe
sophoscleanup.exe	idafserverhostservice.exe	SentinelAgentWorker.exe	sophos ui.exe
iptray.exe	sentinelhelperservice.exe	cloudendpointservice.exe	klnagent.exe
sentinelservicehost.exe	cetasvc.exe	logwriter.exe	sentinelstaticenginescanner.exe
endpointbasecamp.exe	macmnsvc.exe	SentinelUI.exe	wscommunicator.exe
macompatsvc.exe	sepagent.exe	dsa-connect.exe	masvc.exe
sepWscSvc64.exe	responseservice.exe	mbamservice.exe	sfc.exe
epab_svc.exe	mbcloudea.exe	smcgui.exe	fsagentservice.exe
mcsagent.exe	SophosCleanM64.exe	endpoint agent tray.exe	mcsclient.exe
sophosfilescanner.exe	easervicemonitor.exe	mctray.exe	sophosfs.exe
aswtoolssvc.exe	mfeann.exe	SophosHealth.exe	avwrapper.exe
mfemactl.exe	SophosNtpService.exe		

Este programa malicioso utiliza un archivo llamado kill-floor.exe, el cual coloca el controlador aswArPot.sys en un directorio de Windows aparentemente inofensivo, camuflándolo como “ntfs.bin”.

Luego, crea el servicio con el mismo nombre "aswArPot.sys" mediante el Control de servicios (sc.exe) y registra el controlador, lo que le otorga al malware acceso a nivel de kernel (el nivel más alto de privilegio del sistema que le permite finalizar procesos de seguridad críticos y tomar el control del sistema).

El malware monitorea continuamente los procesos activos y los compara con la lista de 142 aplicaciones de seguridad que pretende eliminar. Cuando encuentra una coincidencia, el malware utiliza el controlador Avast Anti-Rootkit para finalizar el proceso de seguridad.



Luego aprovecha la API 'DeviceIoControl' para emitir los comandos IOCTL necesarios para finalizar los procesos.

La función específica “FUN_14001dc80” es la responsable de finalizar los procesos de seguridad. Esta función utiliza funciones estándar del kernel de Windows (KeAttachProcess y ZwTerminateProcess) para llevar a cabo la finalización, enmascarando aún más la actividad maliciosa como operaciones normales del sistema.

Es decir, el controlador de Avast, diseñado para eliminar rootkits maliciosos, desactiva involuntariamente el software de seguridad legítimo. El malware se aprovecha de este controlador confiable para evitar ser detectado y trabajar silenciosamente dentro del sistema.

Entre las soluciones de seguridad afectadas se encuentran productos de reconocidas empresas como:

- McAfee
- Symantec (Broadcom)
- Sophos
- Avast
- Trend Micro
- Microsoft Defender
- SentinelOne
- ESET
- BlackBerry

3. RECOMENDACIONES:

- Establecer reglas capaces de identificar y bloquear componentes en función de sus firmas o hashes.
- Utilizar la política de bloqueo de controladores vulnerables de Microsoft, disponible en Windows 11 2022 y versiones posteriores, y crear listas negras para evitar la instalación de controladores obsoletos.
- Implementar un programa integral de gestión de vulnerabilidades que identifique, priorice y aborde las vulnerabilidades de manera proactiva.

Fuente de Información:	• hxxps://hackread.com/malware-avast-anti-rootkit-driver-bypass-security/ • hxxps://devel.group/blog/cibercriminales-abusan-de-un-controlador-anti-rootkit-de-avast-para-desactivar-defensas/ • hxxps://www.scworld.com/news/avast-anti-rootkit-driver-used-to-seize-control-of-infected-systems • hxxps://www.hfrance.fr/es/los-piratas-informaticos-aprovechan-el-controlador-anti-rootkit-de-avast-para-desactivar-las-protecciones.html

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°272	Fecha: 25-11-2024 Página: 6 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de escalada de privilegios en Cisco Secure Web Appliance		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Cisco Sistemas, Inc. ha publicado una vulnerabilidad de severidad **ALTA** de tipo ejecución con privilegios innecesarios en la interfaz de línea de comandos (CLI) de Cisco AsyncOS para Secure Web Appliance. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante local autenticado ejecutar comandos arbitrarios y elevar privilegios a nivel de root.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-20435 de tipo ejecución con privilegios innecesarios en la CLI de Cisco AsyncOS para Secure Web Appliance, podría permitir que un atacante local autenticado ejecute comandos arbitrarios y eleve privilegios a root.

Esta vulnerabilidad se debe a una validación insuficiente de la entrada proporcionada por el usuario para la CLI. Un atacante podría aprovechar esta vulnerabilidad autenticándose en el sistema y ejecutando un comando creado en el dispositivo afectado. Una explotación exitosa podría permitir al atacante ejecutar comandos arbitrarios en el sistema operativo subyacente y elevar los privilegios a root. Para aprovechar esta vulnerabilidad con éxito, un atacante necesitaría al menos credenciales de invitado.

A. Productos afectados:

- Esta vulnerabilidad afecta a Cisco AsyncOS (anteriores a la versión 15.1) para Secure Web Appliance, tanto a los dispositivos virtuales como a los de hardware.

3. RECOMENDACIÓN:

- Actualizar los paquetes afectados a la última versión disponible que Cisco ha lanzado para abordar esta vulnerabilidad. No existen soluciones alternativas.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-swa-priv-esc-7uHpZsCC

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°272	Fecha: 25-11-2024 Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de omisión de autenticación en el software Apache Answer		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha publicado una vulnerabilidad de severidad **ALTA** de tipo generación de tokens de seguridad incorrectos que afecta al software Apache Answer. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado eludir el proceso de autenticación y obtener acceso no autorizado.

2. DETALLES:

El software Apache Answer es una plataforma de preguntas y respuestas de código abierto diseñada para facilitar el intercambio de conocimientos entre equipos de cualquier tamaño. Sirve para diversos propósitos, incluidos foros comunitarios, centros de ayuda y sistemas de gestión de conocimientos.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-45719 de tipo generación de tokens de seguridad incorrectos en el software Apache Answer, podría permitir a un atacante remoto eludir el proceso de autenticación. La vulnerabilidad existe debido a la generación de tokens de autenticación débiles. Un atacante remoto puede adivinar el token utilizado por la aplicación y obtener acceso no autorizado a la misma.

Esta vulnerabilidad surge del uso de UUID v1 para generar identificadores. El método UUID v1 puede generar tokens predecibles, lo que podría comprometer la confidencialidad del sistema a través de ataques de predicción de tokens.

Hasta el momento, no hay ninguna prueba de concepto (PoC) pública ni evidencia de explotación relacionada con esta vulnerabilidad, pero se recomiendan aplicar medidas proactivas para protegerse contra posibles amenazas.

A. Productos afectados:

- software Apache Answer: versión 0.2.0 - 1.4.0.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la versión 1.4.1 que aborda esta vulnerabilidad.
- Controlar las actividades sospechosas relacionadas con la predicción de tokens y considerar la implementación de medidas de seguridad adicionales, como procesos de autenticación o validación de tokens mejorados.

Fuente de Información:	• hxxp://www.openwall.com/lists/oss-security/2024/11/22/1 • hxxp://lists.apache.org/thread/sz2d0z39k01nbx3r9pj65t76o1hy9491

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°272	Fecha: 25-11-2024 Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en NVIDIA Base Command Manager		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

La empresa NVIDIA Corporation ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo autorización faltante que afecta a NVIDIA Base Command Manager. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado la ejecución de código, realizar un ataque de denegación de servicio (DoS), escalar privilegios, divulgar información y la manipulación de datos.

2. DETALLES:

NVIDIA Base Command Manager es una solución integral de gestión de clústeres diseñada para optimizar la implementación y la gestión de centros de datos de IA. Integra varias funcionalidades, como la gestión de cargas de trabajo y la supervisión de la infraestructura, para mejorar la eficiencia de los sistemas NVIDIA DGX y otro hardware.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-0138 de tipo autorización faltante que afecta a múltiples productos NVIDIA, podría permitir a un atacante remoto no autenticado ejecutar código malicioso, aumentar privilegios y/o provocar una condición de DoS en los sistemas afectados.

NVIDIA Base Command Manager contiene una vulnerabilidad de falta de autenticación en el componente CMDaemon. Una explotación exitosa de esta vulnerabilidad podría provocar la ejecución de código, la denegación de servicio, la escalada de privilegios, la divulgación de información y la manipulación de datos.

A. Productos afectados:

- NVIDIA Base Command Manager, versión 10.24.09.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Actualizar a la versión más reciente de CMDaemon en los nodos principales y en todas las imágenes de software.
- Actualizar los nodos reiniciándolos o resincronizándolos con la imagen del software.
- Implementar la segmentación de la red para limitar el impacto potencial.
- Restringir el acceso a los sistemas NVIDIA solo a usuarios y redes confiables.
- Mantener actualizado todo el software y firmware de NVIDIA con las últimas versiones una vez que estén disponibles.

Fuente de Información:	• hxxps://www.security-database.com/detail.php?alert=CVE-2024-0138 • hxxps://nvidia.custhelp.com/app/answers/detail/a_id/5595

Índice alfabético