Boletín de Ciberseguridad

Fecha de Publicación
10/05/2021 - N.º 7

Mes de Mayo
01/05/2021 - 10/05/2021

Datasec

Índice

Introducción

Por medio de este boletín informativo estaremos destacando de forma quincenal, las noticias más relevantes en el ámbito de la ciberseguridad a nivel regional e internacional.

Las principales categorías de información son: vulnerabilidades tecnológicas, fraudes activos, amenazas por medios informáticos nuevos, así como recomendaciones específicas de prevención. La publicación de dichas noticias dependerá de las importancia y calidad informativa de las mismas.

A su vez se incluyen referencias técnicas y de gestión a los efectos de reducir los riesgos con anticipación y adecuada planificación.

En esta primera quincena del mes de mayo se destacan 6 noticias de relevancia: 3 sobre vulnerabilidades tecnológicas, 2 de fraudes activos y 1 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Se advierte sobre vulnerabilidades en productos de Apple
"Fuentes oficiales han compartido una alerta para aquellos usuarios de Apple y aplicaciones relacionadas con la marca. **Se han descubierto fallas de consideración critica, que, en caso de ser explotadas, los atacantes podrían tomar el control de los equipos de los usuarios.**"

Intento de Fraude mediante página que reemplaza a Paypal
"El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno), **ha identificado la activación de una página fraudulenta que se hace pasar por la plataforma de pagos PayPal, la que podría servir para robar credenciales de usuarios.**"

Falla en Google permite acceder a información de usuarios de apps COVID
"Recientemente ha sido publicado una investigación sobre errores en la implementación de Google de rastreo de COVID en dispositivos que utilizan Android. **Esto puede dejar expuesta información sensible de los usuarios.**"

	Se advierte sobre vulnerabilidades en productos de Apple	CRÍTICO

Descripción

Fuentes oficiales han compartido una alerta para aquellos usuarios de Apple y aplicaciones relacionadas con la marca. **Se han descubierto fallas de consideración critica, que, en caso de ser explotadas, los atacantes podrían tomar el control de los equipos de los usuarios.**

Afectados

iPadOS, versiones de la 14.0 18A373 a la 14.5 18E199.

Apple iOS de la 12.0 16A366 a la 14.5 18E199.

watchOS 7.0 18R382 a la 7.4 18T195.

Estado

Todas estas vulnerabilidades son caracterizadas como de **riesgo crítico y están siendo explotadas activamente.**

La falla permite que un ciberdelincuente pueda ejecutar código remoto arbitrario en el equipo del usuario, esto es debido a un error de límites de la memoria en WebKit.

WebKit es una plataforma para aplicaciones que funciona como base para el navegador web Safari, Epiphany, Maxthon, Midori, QupZilla entre otros.

Remediación / Referencias

Instalar las respectivas actualizaciones desde el sitio web del proveedor.

Por mayor información invitamos a visitar los siguientes sitios:
https://support.apple.com/en-us/HT212336
https://support.apple.com/en-us/HT212341
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00436-01/

python	**Vulnerabilidad crítica afecta a la biblioteca estándar de Python**	IMPORTANTE

Descripción

Se detectó un error critico que afecta a Python, específicamente a la biblioteca que usa el proveedor. Python ofrece a sus usuarios una biblioteca estándar, en esta se puede acceder a funciones, variables, clases, etc. Esto facilita a la comprensión y solución de problemas en matemáticas, estadísticas, compresión de datos, internet, interfaces visuales etc.

“Esta vulnerabilidad provoca un análisis incorrecto de las direcciones IP por parte de la biblioteca estándar ipaddress. Este módulo se encarga de que los desarrolladores puedan crear fácilmente direcciones IP, redes e interfaces. Hay que indicar que una dirección IPv4 puede aparecer en formato decimal, entero, octal o hexadecimal, aunque lo más normal es que aparezca en el primer formato.”

Afectados

Versión Afectada: ipaddress de Python 3.8 a 3.10.

De acuerdo con la especificación original de IETF, para direcciones IP ambiguas, partes de una dirección IPv4 pueden interpretarse como octal si tienen el prefijo "0".

De igual manera 127.0.0.1 no es una dirección IP pública, aunque, su representación ambigua la cambia a una dirección IP pública que lleva a un host completamente diferente.

“Pero, en el caso de la dirección IP de la biblioteca estándar de Python, los ceros iniciales simplemente se eliminarían y descartarían. Una prueba de concepto realizada por los investigadores Sick Codes y Victor Viale muestra que la biblioteca de direcciones IP de Python simplemente descartaría los ceros iniciales. En otras palabras, cuando se analiza mediante el módulo ipaddress de Python, '010.8.8.8' se trataría como '10.8.8.8', en lugar de '8.8.8.8'.”

Estado

"La validación de entrada incorrecta de cadenas octales en Python 3.8.0 a v3.10 stdlib ipaddress permite que atacantes remotos no autenticados realicen ataques SSRF, RFI y LFI indeterminados en muchos programas que dependen de la librería. Por ejemplo, un atacante que envía una dirección IP a una aplicación web que se basa en stdlib ipaddress, podría causar SSRF al ingresar datos de entrada octal. Por ejemplo, un atacante puede enviar 010.8.8.8, que es 8.8.8.8, sin embargo, la dirección IP incorporada de Python evaluará esto como 10.8.8.8."

"Aquí llega el problema con los ceros a la izquierda. Es lo mismo que ocurría con la biblioteca netmask. La manera en la que gestiona esa IP cambia al agregar un valor cero antes de la IP en formato decimal. Lo que ocurre con la vulnerabilidad de Python es que los ceros a la izquierda los descartaría."

El problema con esta vulnerabilidad en la validación IP, es que deja al usuario expuesto a ataques remotos. Un ciberdelincuente sin autorización podría ponerse del lado del servidor para llevar a cabo solicitudes falsas. Esto repercute en cientos de aplicaciones que se basan en el lenguaje de programación Python.

Remediación / Referencias

Se espera a que la falla pueda ser solucionada mediante las actualizaciones correspondientes, pero como señalan los especialistas, no es común administrar direcciones IP utilizando ceros a la izquierda, por lo que es difícil que se ejecute el exploit.

Por mayor información acceder a:
https://blog.segu-info.com.ar/2021/05/vulnerabilidad-en-la-validacion-de-ip.html
https://www.bleepingcomputer.com/news/security/python-also-impacted-by-critical-ip-address-validation-vulnerability/

Pulse Secure	Se publican vulnerabilidades zero-day en VPN Pulse Secure	IMPORTANTE

Descripción

El Equipo de Respuesta ante Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN-CERT, alerta sobre una vulnerabilidad de tipo zero-day que afecta a VPN Pulse Secure.

Se cree que el programa que ofrece el servicio de redes virtual privadas (VPN) de Pulse Secure, presenta fallas de tipo Dia-Cero, provocando varios incidentes de seguridad.

Pulse Secure es una VPN basada en SSL corporativo que requiere una Pulse Connect Secure SSL.

Pulse Secure crea una conexión segura a Pulse Connect Secure corporativa SSL VPN gateway para proporcionar acceso instantáneo a las aplicaciones empresariales y datos desde cualquier lugar en cualquier momento.

Afectados

Las versiones afectadas de Pulse Connect Secure son las siguientes:

9.0R3, 9.0R3.1, 9.0R3.2, 9.0R3.4 y 9.0R3.5,
9.0R4 y 9.0R4.1.
9.0R5.0.
9.0R6.0.
9.1R1.
9.1R2.
9.1R3.
9.1R4, 9.1R4.1, 9.1R4.2 y 9.1R4.3.
9.1R5.
9.1R6.
9.1R7.
9.1R8, 9.1R8.1, 9.1R8.2 y 9.1R8.4.
9.1R9, 9.1R9.1 y 9.1R9.2.
9.1R10, 9.1R10.0 y 9.1R10.2.
9.1R11, 9.1R11.0, 9.1R11.1 y 9.1R11.3.

Estado

Hasta el momento se ha confirmado que, desde hace unos meses, al menos dos grupos de ciberdelincuentes han puesto en marcha la explotación activa de estas vulnerabilidades en Pulse Secure.

Mediante la ejecución de código malicioso y binarios modificados, comprometieron muchos dispositivos, recopilando información de credenciales de usuario para el inicio del programa.

Malware Identificados: SLOWPULSE, RADIALPULSE, PULSEJUMP y THINBLOOD.

“SLOWPULSE: las interacciones de este malware se pueden detectar mediante la correlación de registros entre los servidores de autenticación responsables de la autenticación LDAP y el servidor VPN. Las credenciales de inicio de sesión se encuentran en el archivo /home/perl/PAUS.pm”

“RADIALPULSE y PULSEJUMP: En el caso de estos malware, se puede verificar mediante la existencia de los archivos utilizados para registrar las credenciales.”

Remediación / Referencias

Si ha sido afectado por estas vulnerabilidades, instamos a entrar al siguiente link: https://support.pulsesecure.net/support/support-contacts/

Además, existe una herramienta de análisis para garantizar la integridad total del software Pulse Connect Secure.

Entrar al siguiente enlace para acceder a la herramienta Pulse Connect Secure (PCS) Integrity Assurance: https://kb.pulsesecure.net/pkb_mobile#article/l:en_US/KB44755/s

Se exhorta a los usuarios y administradores de sistemas que instalen las actualizaciones, cuando sean lanzadas por el proveedor.

Por mayor información invitamos a visitar los siguientes sitios:
https://www.ccn-cert.cni.es/seguridad-al-dia/alertas-ccn-cert/10958-ccn-cert-al-05-21-vulnerabilidad-zero-day-vpn-pulse-secure.html

PayPal	**Intento de Fraude mediante página que reemplaza a Paypal**	IMPORTANTE

Descripción

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno), **ha identificado la activación de una página fraudulenta que se hace pasar por la plataforma de pagos PayPal, la que podría servir para robar credenciales de usuarios.**

Este fraude puede repercutir en la imagen institucional de la empresa, generando un gran daño a la marca y a los usuarios que la utilizan.

URL sitio falso
https://prosemec[.]cl/secure/signin/index.php

Certificado Digital
Fecha Válida: 02-03-2021
Fecha Término: 01-06-2021
Emitido: cPanel, Inc. Certification Authority

Datos Alojamiento
IP [131.72.236.173]
Número de Sistema Autónomo (AS): 263753
Etiqueta del Sistema Autónomo: GONZALEZ ULLOA JUAN CARLOS
País: CL
Registrador: LACNIC

Datos del Dominio
Nombre de Dominio :prosemec[.]cl
Creado: 18-11-2016
Expira:14-12-2021
Información del Registrador: NIC Chile
Name Server: ns53.benzahosting.cl
ns54.benzahosting.c

Afectados

Paypal cuenta con más de 200 millones de usuarios en todo el mundo, siendo una de las opciones más elegidas para realizar pagos mediante internet.

Estado

"La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares. "

"Estos casos de fraude no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado fraude, para construir el engaño. "

Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

Remediación / Referencias

No abrir correos ni mensajes de dudosa procedencia.
Desconfiar de los enlaces y archivos en los mensajes o correo.
Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet

Prestar atención en los detalles de los mensajes o redes sociales
Evaluar el bloqueo preventivo de los indicadores de compromisos.
Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
Revisar los controles de seguridad de los AntiSpam y SandBoxing.
Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
Visualizar los sitios web que se ingresen sean los oficiales.

Por mayor información al respecto se puede acceder a:
https://www.csirt.gob.cl/alertas/8ffr21-00942-01/

El informe oficial publicado por el CSIRT del Gobierno de Chile está disponible en el siguiente enlace:
https://www.csirt.gob.cl/media/2021/04/8FFR21-00942-01.pdf

	**Malware RotaJakiro afecta a Linux**	IMPORTANTE

Descripción

A través de un backdoor el malware RotaJakiro ha estado afectando a Linux durante años, mediante esta puerta trasera **el intruso puede realizar descargas no autorizadas, también insertar código tomando así el control del equipo vulnerado.**

Como todos los malware ha sido diseñado para actuar de manera silenciosa, pero en especial se destaca por ser muy difícil de detectar en el sistema.

Afectados

“A nivel funcional, RotaJakiro primero determina si el usuario es root o no en tiempo de ejecución, con diferentes políticas de ejecución para diferentes cuentas, luego analiza los recursos sensibles relevantes, al tiempo que adopta las medidas necesarias para garantizar su persistencia y procede a enmascarar los procesos con el fin de pasar desapercibido.”

Después de ser ejecutado busca establecer comunicación con el servidor de comando y control, a la espera de recibir instrucciones de que hacer en el dispositivo infectado.

Estado

"RotaJakiro admite un total de 12 funciones, tres de las cuales están relacionadas con la ejecución de complementos específicos. Desafortunadamente, no tenemos visibilidad de los complementos y, por lo tanto, no conocemos su verdadero propósito" agregaron los investigadores.”

La explotación aún sigue activa, además debido a que tiene un bajo perfil y poca visibilidad, se cree que es un malware que se ejecuta de manera selectiva y no masiva. Esto hace pensar que se usa para exfiltrar información.

Remediación / Referencias

Todos los sistemas operativos pueden ser proclives a ser vulnerados y por más que las organizaciones buscar mediante actualizaciones constantes poder solucionar estas fallas, los cibercriminales encuentran la manera de vulnerarlos, por lo que se exhorta a estar atentos y precavidos.

Por mayor información al respecto se puede acceder a:
https://wwwhatsnew.com/2021/04/29/rotajakiro-el-virus-para-linux-que-ha-sido-invisible-durante-anos/
https://blog.netlab.360.com/stealth_rotajakiro_backdoor_en/

Falla en Google permite acceder a información de usuarios de apps COVID

PREVENCIÓN

Descripción

Recientemente ha sido publicada una investigación sobre errores en la implementación de Google de rastreo de COVID en dispositivos que utilizan Android. **Esto puede dejar expuesta información sensible de los usuarios.**

"La implementación de Google fue insuficiente, ya que los datos privados de dicha aplicación quedaban registrados en el archivo interno del dispositivo, donde eran accesibles para el resto de apps preinstaladas. Es decir, dicho error permitía conocer la identidad del usuario, localización, contactos y si había dado positivo en coronavirus."

Independientemente que el dispositivo utilice iOS o Android, lo que hace es conectaste de manera constante con los equipos de otros usuarios que se encuentran cerca, asignándoles una única clave. Si pasados los 14 días alguna de estas personas da positivo de COVID – 19, se genera una alerta para quienes estuvieron en contacto cercano.

Afectados

Los usuarios de Android son los afectado por esta falla. Se estima que en el mundo hay 2.500 millones de dispositivos activos de Android.

Vector de Ataque

“En concreto, el problema está en las apps preinstaladas en Android, las que ya vienen en el móvil cuando las compramos; afecta no sólo a las apps de Google que vienen en casi todos los dispositivos, sino también a las apps que son instaladas por fabricantes y compañías como parte de promociones, llamadas comúnmente "bloatware".”

Los especialistas determinaron que el sistema de Google puede dar el acceso a registros privados relacionados con el rastreo de COVID a determinadas aplicaciones.

Remediación / Referencias

Google confirmó estar informado del error, y que ya está poniendo en práctica el lanzamiento de parches para la mitigación del problema.

“Hace ya un año que Google y Apple anunciaron una alianza histórica contra la mayor pandemia de las últimas décadas, la de la COVID-19. Ambas empresas dejaron atrás su rivalidad para crear un sistema único de rastreo de contacto, "contact tracing" para evitar la propagación del nuevo coronavirus.”

Por mayor información al respecto se puede acceder a:
https://blog.segu-info.com.ar/2021/04/error-de-google-permite-acceder.html
https://www.20minutos.es/tecnologia/ciberseguridad/un-error-de-google-permitia-acceder-a-informacion-privada-de-usuarios-de-la-app-radar-covid-4676291/

Conclusiones

Las recomendaciones generales siguen estando enfocadas en los posibles riesgos que se puedan generar a nivel de las conexiones remotas de los teletrabajadores, tanto a nivel de los conectores VPN que dispongamos, los mismos se recomienda tanto actualizarlos como contar con configuraciones seguras que eviten y/o puedan evaluar el estado de salud general de los endpoints o sistemas que se conectan a la VPN.

Es decir, es muy valioso poder contar en estas situaciones con validadores de higiene general de equipamientos remotos, tanto a nivel de que los sistemas operativos estén actualizados y con los parches de seguridad al día, así como también que los controles de seguridad tales como los antivirus estén también habilitados y funcionando. Esto previene en gran medida los posibles abusos o compromisos que se puedan generar a nivel de los usuarios remotos a los cuales le damos acceso a la red informática de la organización. Existen varias soluciones técnicas a este nivel tanto como Fortinet con su Forticlient Health Check como soluciones tales como Duo Security Device Health, entre otros de otros fabricantes.

Esto mejorará la postura de ciberseguridad, también habilitar la autenticación con dobles factores aumenta en gran medida la pérdida de accesos de estos usuarios remotos y refuerza mucho la protección.

Esperamos que sus datos sigan protegidos, para cualquier apoyo quedamos atentos desde los diferentes equipos de trabajo de Datasec.