Boletín de Ciberseguridad

Fecha de Publicación
22/11/2021 - N.º 21

Mes de noviembre
08/11/2021 - 22/11/2021

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 segunda quincena del mes de noviembre se destacan 6 noticias de relevancia: 2 sobre vulnerabilidades tecnológicas, 2 de fraudes activos y 2 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Dos Zero-Day explotadas activamente en Excel y Exchange Server

Microsoft ha publicado su actualización de seguridad mensual y dentro de esta se encuentran dos vulnerabilidades que están siendo explotadas activamente en la naturaleza.

MasterFred: malware para Android dirigido a usuarios de Netflix, Instagram y Twitter

Un nuevo malware para Android conocido como MasterFred utiliza superposiciones de inicio de sesión falsas para robar la información de las tarjetas de crédito de los usuarios de Netflix, Instagram y Twitter.

Fin del servicio para Windows 10 versión 2004

Microsoft ha lanzado un recordatorio para aquellos que aún ejecutan la actualización de Windows 10 de mayo de 2020 (versión 2004) en sus dispositivos. El sistema operativo cumplirá su fecha límite de fin de servicio el 14 de diciembre de 2021.

	**Dos Zero-Day explotadas activamente en Excel y Exchange Server**	CRÍTICO

Descripción

Microsoft ha publicado su actualización de seguridad mensual y dentro de esta se encuentran dos vulnerabilidades que están siendo explotadas activamente en la naturaleza.

Afectados

Microsoft Exchange Server
Microsoft Excel

Estado

En el Sistema de Puntuación de Vulnerabilidad Común (CVSS), uno de los fallos tiene una puntuación de 8,8 sobre 10 y puede ser explotado mediante previa autenticación en el sistema por parte del atacante y está relacionada con una falla de ejecución remota de código posterior a la autenticación en Microsoft Exchange Server.

La otra falla calificada como importante tiene una puntuación CVSS de 7,8 y afecta tanto a las versiones de Windows como de Mac. Se trata de una vulnerabilidad de evasión de seguridad que permite la carga de código malicioso con sólo abrir un archivo Excel. La

explotación exitosa de esta vulnerabilidad requiere que un usuario abra el archivo malicioso de Excel. Si se abre, un atacante sin privilegios tendrá acceso total de lectura y escritura a todos los recursos del componente afectado.

Remediación / Referencias
Aplicar las ultimas actualizaciones publicadas por Microsoft que mitigan estas vulnerabilidades.

Por mayor información acceder a:
https://blog.segu-info.com.ar/2021/11/actualizaciones-de-seguridad-de.html

	Vulnerabilidades de Chrome están siendo explotadas activamente por atacantes	CRÍTICO

Descripción
Google ha publicado la versión 95.0.4638.69 de Chrome para Windows, Mac y Linux con el fin de solucionar dos vulnerabilidades de día cero.

Afectados
Google Chrome anteriores a 95.0.4638.69.

Estado
La primera vulnerabilidad tiene una calificación de gravedad alta y se describe como Validación insuficiente de la entrada que no es de confianza en Intents.

El segundo fallo tiene una gravedad alta y corresponde a un error de implantación inapropiada en el motor de JavaScript de Chrome V8.

Por el momento, Google aún no ha informado sobre cómo los actores de amenazas explotan las vulnerabilidades en los ataques.

Remediación / Referencias
Instalar las respectivas actualizaciones entregadas por el proveedor.

Puedes acceder a toda la información en el siguiente enlace:
https://www.welivesecurity.com/la-es/2021/10/29/google-chrome-dos-nuevas-zero-day-explotadas-activamente/

MasterFred para Android dirigido a usuarios de Netflix, Instagram y Twitter

IMPORTANTE

Descripción

Un nuevo malware para Android conocido como MasterFred utiliza superposiciones de inicio de sesión falsas para robar la información de las tarjetas de crédito de los usuarios de Netflix, Instagram y Twitter.

Afectados

Usuarios de Netflix, Instagram y Twitter con dispositivos Android.

Estado

Se trata de un nuevo troyano que se cuela en los dispositivos Android con el objetivo de robar información financiera de las víctimas.

Una vez instalada la aplicación falsa, el malware le pide a los usuarios que le otorguen la capacidad de usar el servicio de accesibilidad de Android lo que le permitirá obtener un control total sobre el dispositivo infectado ya sea por medio descargas y ejecución de otras cargas útiles, de comandos y operaciones remotas sin el permiso del usuario.

Lo que diferencia a MasterFred de otros tipos de ataques similares es que utiliza superposiciones HTML para mostrar los formularios de inicio de sesión falsos que permitirán recopilar la información de la víctima.

Este tipo de software malicioso suele llegar a través de aplicaciones falsas que instalamos en el dispositivo. Simulan ser legítimas y con una apariencia que puede hacer que la víctima llegue a iniciar sesión o dar información.

Expertos en ciberseguridad indicaron que al menos una de las aplicaciones maliciosas que integran MasterFred ha estado en Google Play.

Una vez robada la información, se utiliza la red Tor a través de la Dark Web Onion.ws. para entregar la información a los servidores de la red bajo el control de su operador.

Remediación / Referencias

- Contar con programas de seguridad.
- Tener las últimas versiones instaladas.
- Descargar siempre aplicaciones de tiendas oficiales.

Por mayor información al respecto se puede acceder a:
https://cybersecuritynews.es/masterfred-el-malware-que-roba-datos-bancarios-de-netflix/

Atacantes roban códigos de verificación con bots de voz

IMPORTANTE

Descripción

Ciberdelincuentes se dirigen a los usuarios de plataformas como Amazon o PayPal para robar las contraseñas temporales que los usuarios reciben en sus teléfonos, utilizando bots de voz y así acceder a sus cuentas.

Afectados

Usuarios de Amazon, PayPal, Coinbase u otro banco.

Estado

Piratas informáticos han deducido una forma de robar códigos de autenticación de dos factores y contraseñas de un solo uso utilizando bots de voz para engañar a los usuarios y así ingresar en sus cuentas para robar dinero.

Esto es posible debido a un nuevo tipo de bots personalizables que realizan llamadas automáticas con el único objetivo de robar las contraseñas temporales que los usuarios reciben en sus teléfonos.

Bot es mucho más sofisticado y hará creer que estás hablando con el sistema de seguridad automatizado del servicio que los hackers quieren penetrar.
Los atacantes con datos como nombre real, dirección de correo electrónico y número de teléfono pueden utilizarlos para determinar si un usuario tiene una cuenta de PayPal, por ejemplo, con esa dirección.
Procedimiento que puede aplicarse a cualquier tipo de cuenta en Internet.

Una vez que encuentran una coincidencia, pueden introducir el número de teléfono de la víctima en un bot adaptado a ese servicio.

La razón por la que las victimas reciben un código a través de un mensaje de texto en su teléfono es que el hacker ha intentado entrar en su cuenta, sabiendo perfectamente que no podrá hacerlo. El bot hace creer que es un servicio como PayPal el que genera el código 2FA/OTP único. Y no tendrán forma de saber que es un ciberdelincuente quien está realizando el ataque.

Los bots que se emplean para las estafas pueden conseguirse en chats de Telegram o en Discord a un precio que va desde los 100 hasta los 1000 dólares.
Estas nuevas formas de cometer fraude cada vez son más conocidas, por lo que es necesario que los usuarios estén al tanto de la existencia de esta modalidad y tener claro que no se debe compartir los códigos 2FA u OTP con nadie.

Remediación / Referencias

Accede a la nota completa aquí:
https://www.welivesecurity.com/la-es/2021/11/17/bots-de-voz-robar-codigo-verificacion-mediante-llamadas/

Windows 10	**Fin del servicio para Windows 10 versión 2004**	PREVENCIÓN

Descripción

Microsoft ha lanzado un recordatorio para aquellos que aún ejecutan la actualización de Windows 10 de mayo de 2020 (versión 2004) en sus dispositivos. El sistema operativo cumplirá su fecha límite de fin de servicio el 14 de diciembre de 2021.

Estado:

Esto se aplica a las siguientes ediciones de Windows 10 lanzadas en mayo de 2020:

- Windows 10 Home, versión 2004
- Windows 10 Pro, versión 2004
- Windows 10 Pro Education, versión 2004
- Windows 10 Pro para estaciones de trabajo, versión 2004
- Windows 10 Enterprise, versión 2004
- Windows 10 Education, versión 2004
- Windows 10 IoT Enterprise, versión 2004

A partir del 14 de diciembre, los equipos que ejecuten esa versión dejarán de recibir las actualizaciones mensuales de seguridad y calidad.

Una vez que Microsoft deje de dar soporte a las ediciones expuestas anteriormente, la compañía seguirá proporcionando actualizaciones para las siguientes versiones:

- La actualización de Windows 10 de mayo de 2021 (versión 21H1).
- La próxima actualización de Windows 10 de noviembre de 2021 (versión 21H2).
- Windows 11 si su dispositivo cumple con los requisitos mínimos del sistema.

Según el último informe de AdDuplex, Windows 10 2004 es la tercera versión de Windows más popular del mundo, con un 14,1% del mercado total. Windows 10 20H2 (actualización de octubre de 2020) tiene el 36,1%, y Windows 10 21H1 ocupa el primer lugar con el 38,1%.

Referencias

Por mayor información:
https://www.welivesecurity.com/la-es/2021/11/12/diciembre-windows-10-2004-dejaran-recibir-actualizaciones/
https://docs.microsoft.com/en-US/lifecycle/faq/windows

npm	**Malware encontrado en el paquete NPM con millones de descargas semanales**	PREVENCIÓN

Descripción

Descubiertos dos paquetes pertenecientes a NPM que contienen malware requieren volver a versiones anteriores. Los paquetes comprometidos tienen alta popularidad, contando con unos 22 millones de descargas semanales.

Estado:

NPM es el sistema de gestión de paquetes o software de código abierto por defecto para Node.js. Las dos bibliotecas pirateadas y modificadas son:

- COA (comando-opción-argumento) que es un analizador de opciones de línea de comandos que tiene como objetivo aprovechar al máximo la formalización de la API de su programa. Todas las versiones de coa que comienzan con 2.0.3 y superiores (2.0.3, 2.0.4, 2.1.1, 2.1.3, 3.0.1 y 3.1.3) se ven afectadas.

- Rc, que es un cargador de configuración.

Este paquete debe considerarse comprometido en cualquier máquina que lo tenga instalado o en ejecución. Todas las claves de esa computadora deben rotarse a otra diferente lo antes posible. El paquete debe desinstalarse, pero debido a que el control total de la computadora

puede haber sido otorgado a una entidad externa, ninguna garantía al hacerlo eliminará cualquier software peligroso que resulte de su instalación.

Remediación / Referencias

- Las versiones comprometidas para “rc” son 1.2.9, 1.3,9 y 2.3.9, por lo que se recomienda volver a la versión más actualizada no comprometida, la 1.2.8.

- Respecto a “coa”, desde la versión 2.0.3 hasta la versión 3.1.3 contiene rastro de malware. Es por ello que se recomienda volver a la versión anterior a estas, la 2.0.2.

- Así como también habilitar la doble autenticación en NPM.

Para saber más invitamos a visitar el siguiente sitio:
https://blog.segu-info.com.ar/2021/11/paquetes-npm-modificados-e-infectados.html

Conclusiones

A nivel global se sigue priorizando la seguridad de la información debido a que es valiosa para las empresas y también para los adversarios.
Vemos como estos evolucionan también con las nuevas tecnologías, y que la alfabetización digital y sobre todo el manejo de la información de cualquier tipo es cada vez más necesario para las personas de cualquier sociedad moderna.
Es por ello por lo que la concientización efectiva es importante se aborde desde diversas áreas, como las nuevas técnicas, tácticas y procedimientos que son utilizados permitiendo así comprobar y garantizar medios de confianza efectivos en cada caso.

Tenemos, por ejemplo, las noticias que publicamos en dónde se utilizan herramientas de software sencillas de adquirir y utilizar, que permiten falsear conversaciones con entidades bancarias y demás organizaciones que se están automatizando con voces de robots.
Similares aspectos observamos con el aumento de los videos de rostros, así que tanto estos, como los sonidos de voces humanas, que son posibles falsearlas llegando a ser en varios casos muy parecidos a los originales, posibilita, por ejemplo, ser utilizado por atacantes para simular la voz de algún tomador de decisiones generando una gran cantidad de fraudes.

Cada vez más toda la información que manejamos y recibimos de forma periódica entra en un proceso parecido al método científico en dónde la información debe ser verificada entre varias vías de confianza como: puntaje del chofer o del servicio brindado por la plataforma, doble factor de autenticación en un login, llaves criptográficas para verificar la integridad de un e-mail, revisores de fake news, etc.

El conocimiento sobre seguridad de la información permite facilitarlo ya que contempla las mejores prácticas estudiadas e implementadas por las organizaciones para la protección efectiva.

Desde Datasec seguimos haciendo nuestra parte para seguir defendiendo lo que consideramos valioso: la información en cualquier estado.