Boletín de Ciberseguridad

Fecha de Publicación
12/09/2022- N.º 42

Mes de Septiembre
29/08/2022 -12/09/2022

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 la 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 Septiembre se destacan 6 noticias de relevancia: 3 sobre vulnerabilidades tecnológicas y 3 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Hackers apuntan a funcionarios gubernamentales en Europa, América del Sur y Medio Oriente.

Ciberdelincuentes con sede en China, infectan a través de un malware conocido como PlugX a funcionarios gubernamentales en Europa, América del Sur y Europa.

Servicios populares siguen permitiendo el uso de contraseñas débiles

Un informe reciente reveló que varios servicios populares utilizan políticas de contraseña particularmente débiles en la parte de su sitio web orientada al cliente.

Google parchea vulnerabilidad en Chrome

Actualización lanzada para Google Chrome, corrige vulnerabilidad zero-day en el navegador.

	Hackers apuntan a funcionarios gubernamentales en Europa, América del Sur y Medio Oriente.	CRÍTICO

Descripción

Ciberdelincuentes con sede en China, infectan a través de un malware conocido como PlugX a funcionarios gubernamentales en Europa, América del Sur y Europa.

Estado

Expertos en seguridad cibernética identificaron las intrusiones en junio y julio de 2022, se estima que el grupo de actores el cual se encuentra activo desde al menos julio de 2018, es patrocinado directamente por el estado, y aprovecha la combinación de herramientas patentadas y disponibles públicamente para comprometer y recopilar datos de sus objetivos.

Si bien el grupo de atacantes es conocido bajo diferentes nombres, su principal herramienta de elección es PlugX, un troyano de acceso remoto que se ha compartido ampliamente entre colectivos adversarios chinos. Se trata de un malware modular que se pone en contacto con un servidor de comando y control (C2) para realizar tareas y puede descargar complementos adicionales para mejorar su capacidad más allá de la recopilación de información básica.

Las cadenas de ataque distribuyen archivos RAR que contienen **un archivo de acceso directo de Windows (.LNK) disfrazado de documento PDF**, que se abre y ejecuta un archivo legítimo presente en una carpeta oculta anidada incrustada en el archivo.

Esto allana el camino para colocar un documento señuelo, mientras que la carga útil de PlugX configura la persistencia en el host infectado.

Remediación / Referencias

Como precaución se sugiere que las organizaciones en las regiones geográficas de interés para China, monitoreen de cerca las actividades de este grupo, especialmente agencias gubernamentales o asociadas a ellas.

Por mayor información acceder a:
https://thehackernews.com/2022/09/chinese-hackers-target-government.html

	**Instagram es multada por violar la privacidad de los menores**	CRÍTICO

Descripción

Instagram ha sido multado por infringir el Reglamento General de Protección de Datos (RGPD).

Estado

La Comisión Irlandesa de Protección de Datos (DPC) impuso una multa de 405 millones de euros a la red social tras descubrir que mostraba datos personales de menores. La sanción es la tercera que recibe Meta y una de las más altas que otorga el regulador irlandés.

La multa a Instagram llega tras una investigación de casi dos años realizada por la DPC. En octubre de 2020, el organismo de control irlandés abrió dos investigaciones contra la red social tras conocer que Instagram reveló datos de contacto de millones de menores. Científicos publicaron los resultados del análisis realizado en más de 200.000 cuentas en varios países, incluidos los que se rigen por el RGPD.

Fue posible extraer información personal de menores, como números de teléfono o direcciones de correo electrónico. Los científicos aprovecharon una vulnerabilidad de Instagram que expone información personal cuando una cuenta cambia de perfil personal a perfil profesional.

Los expertos indicaron que los datos se filtraron durante meses y denunció el incidente a Instagram. A pesar de la gravedad de la situación, la empresa no tomó ninguna medida para evitarlo y simplemente eliminó la información de contacto del código HTML de la página de perfil.

Tras los hallazgos, se presentó la denuncia ante el DPC argumentando que Instagram podría haber expuesto los datos personales de más de 5 millones de usuarios menores de edad. Según el artículo 8 del RGPD, el tratamiento de datos personales se considera lícito a partir de los 16 años, mientras que los menores necesitan la autorización de sus padres o tutores. La edad mínima para tener una cuenta de Instagram es de 13 años.

Remediación / Referencias

Lo interesante aquí es que Facebook trabajó en una versión de Instagram para niños menores de 13 años al mismo tiempo que no hizo nada para evitar que su aplicación principal filtrara la información sensible de estos usuarios. De cualquier manera, Meta aún se encuentra argumentando su caso.

Puedes acceder a toda la información en el siguiente enlace:
https://edition.cnn.com/2022/09/06/tech/instagram-fine-teens-privacy/index.html

	**Servicios populares siguen permitiendo el uso de contraseñas débiles**	CRÍTICO

Descripción

Un informe reciente reveló que varios servicios populares utilizan políticas de contraseña particularmente débiles en la parte de su sitio web orientada al cliente.

Estado

Shopify utilizado por más de 3,9 millones de sitios web activos en todo el mundo, y Zendesk con más de 170.00 clientes, bloquean el 2% de las contraseñas comprometidas. Ofrecen autenticación de dos factores (2FA), sin embargo, no es un requisito al crear una cuenta, una contraseña con al menos 5 caracteres y no realiza una verificación de las contraseñas ingresadas.

Trello con más de 7.4 millones de usuarios globales, previene menos del 13% de sus contraseñas comprometidas, ofreciendo 2FA (sin ser requisito), no realiza una verificación de contraseña comprometida y se exige que la misma tenga al menos 8 caracteres.

Stack Overflow bloquea el 46% de las contraseñas comprometidas. No ofrece 2FA ni realiza una verificación de contraseña comprometida, sin embargo, las contraseñas exigidas deben contener al menos ocho caracteres, incluidos al menos 1 letra y 1 número.

Mailchimp bloquea el 98% de las contraseñas comprometidas conocidas. A pesar de que no requiere 2FA, esto se debe a la aplicación de una política de contraseñas compleja: al menos 8 caracteres, 1 caracter especial, 1 número, 1 letra mayúscula, 1 letra minúscula.

Un estudio reciente hace eco de los peligros de usar contraseñas débiles. El estudio examina la cantidad de tiempo que se requeriría para descifrar por fuerza bruta contraseñas de varias longitudes y con diferentes niveles de complejidad.

Una contraseña de cinco caracteres se puede descifrar instantáneamente, independientemente de su complejidad. Dada la facilidad con la que se pueden descifrar contraseñas más cortas utilizando la fuerza bruta, lo ideal es que las organizaciones requieran contraseñas complejas que tengan al menos 12 caracteres de longitud.

Remediación / Referencias

El objetivo de una buena política de contraseñas está destinado a hacer que la red y credenciales en los diferentes servicios sea más segura, por lo cual recomendamos tener en cuenta los siguientes puntos:

- Fortaleza y longitud: es necesario crear claves que contengan mayúsculas, minúsculas, números y símbolos especiales. Además de ser lo más largas posibles con un mínimo de 12 caracteres.
- Caducidad: deben contar con una fecha de vencimiento para que se cambien con regularidad.
- Historial de contraseñas: las contraseñas utilizadas anteriormente, deben de ser almacenadas para que los usuarios no puedan reutilizarlas.
- El cambio de contraseña debe de estar disponible en cualquier momento, pero deben estar implementadas medidas de seguridad como la autenticación de dos factores.

Por mayor información:
https://thehackernews.com/2022/09/shopify-fails-to-prevent-known-breached.html

	Google parchea vulnerabilidad en Chrome	PREVENCIÓN

Descripción

Actualización lanzada para Google Chrome, corrige vulnerabilidad zero-day en el navegador.

Estado

Por su parte, la compañía confirmó que está al tanto de la existencia de un exploit para este fallo que está siendo utilizado por cibercriminales en ataques, aunque no dio detalles de las características de los mismos.

Se trata de una vulnerabilidad de validación de datos insuficiente en Mojo, una colección de librerías runtime utilizadas en Chromium, que impulsa gran parte del código detrás del navegador, la cual también podría explotarse en Microsoft Edge, Brave, Opera, and Vivaldi.

Esta zero-day es la séptima que Google repara en lo que va de 2022. Vale la pena recordar que en 2021 la compañía reparó un total de 17 vulnerabilidades que estaban siendo utilizadas por atacantes previo a que fueran reportadas.

Remediación / Referencias

Google no ha proporcionado detalles exactos de a qué se refiere la actualización de seguridad, indicando que el acceso a los detalles de errores y enlaces puede mantenerse restringido hasta que la mayoría de los usuarios se actualicen con una solución.

Con esta actualización la última versión de Chrome es la 105.0.5195.102 para Windows, Mac y Linux.

Para más información acceder a: https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop.html
https://blog.segu-info.com.ar/2022/09/google-soluciona-vulnerabilidad-critica.html

ATLASSIAN Bitbucket	**Vulnerabilidad crítica en Bitbucket permite el secuestro de servidores**	PREVENCIÓN

Descripción

Vulnerabilidad crítica en la API de Atlassian Bitbucket Server y Data Center podría permitir que un atacante no autorizado ejecute malware de forma remota y vea, cambie e incluso elimine datos almacenados en repositorios.

Estado

Investigadores de seguridad descubrieron e informaron la vulnerabilidad a través del programa de recompensas por errores de Atlassian.

La empresa ha corregido la intrusión de seguridad, que está presente en las versiones 7.0.0 a 8.3.0 del software, inclusive. Afortunadamente, no hay hazañas conocidas al momento.

La vulnerabilidad permite a un atacante con acceso a un repositorio público o con permisos de lectura a un repositorio privado de Bitbucket, ejecutar código arbitrario enviando una solicitud HTTP maliciosa.

Atlassian recomienda que las organizaciones actualicen sus instancias a una versión fija, y aquellas con nodos de Bitbucket Mesh configurados también deberán actualizarlos. Hay una matriz de compatibilidad para ayudar a los usuarios a encontrar la versión de Mesh que sea compatible con la versión de Bitbucket Data Center.

Y si necesita posponer una actualización de Bitbucket, Atlassian recomienda desactivar los repositorios públicos a nivel mundial como una mitigación temporal. Esto cambiará el vector de ataque de un ataque no autorizado a uno autorizado. Sin embargo, esto no puede considerarse una mitigación completa, ya que un atacante con una cuenta de usuario aún podría tener éxito.

Remediación / Referencias

Recomendamos ingresar a Bitbucket Support para obtener información detallada sobre la vulnerabilidad, el alcance del parche, así como la matriz de compatibilidad para usuarios de Bitbucket Mesh.

Por mayor información acceder a:
https://confluence.atlassian.com/bitbucketserver/bitbucket-server-and-data-center-advisory-2022-08-24-1155489835.html

CISCO	**Cisco parchea vulnerabilidades encontradas en diversos productos**	PREVENCIÓN

Descripción

Vulnerabilidad crítica en la API de Atlassian Bitbucket Server y Data Center podría permitir que un atacante no autorizado ejecute malware de forma remota y vea, cambie e incluso elimine datos almacenados en repositorios.

Estado

Cisco lanzó parches para abordar tres fallas de seguridad que afectan a sus productos, incluida una debilidad de alta gravedad revelada en NVIDIA Data Plane Development Kit (MLNX_DPDK) a finales del mes pasado.

La primera vulnerabilidad con un puntaje CVSS: 8.6, deriva de la falta de un manejo adecuado de errores en la pila de red de DPDK, lo que permite que un adversario remoto active una condición de denegación de servicio (DoS) y cause un impacto en integridad y confidencialidad de los datos.

Si se observa una condición de error en la interfaz del dispositivo, el dispositivo puede recargarse o no recibir tráfico, lo que resulta en una condición de denegación de servicio (DoS).

Cisco investigó su línea de productos y determinó que los siguientes servicios se vieron afectados por el error:

- Software perimetral Cisco Catalyst 8000V
- Dispositivo virtual de seguridad adaptable (ASAv), y
- Firewall seguro Threat Defense Virtual (anteriormente FTDv)

La segunda vulnerabilidad resuelta, con un puntaje CVSS: 7.5, se encuentra en su software Cisco SD-WAN vManage que podría permitir que un atacante adyacente no autenticado que tenga acceso a la red lógica VPN0 también acceda a los puertos del servicio de mensajería en un sistema afectado.
La explotación exitosa de la falla podría permitir que el atacante vea e inyecte mensajes en el servicio de mensajería, lo que puede causar cambios en la configuración o hacer que el sistema se vuelva a cargar.

La tercera falla remediada por Cisco con un puntaje CVSS: 4.3, es una vulnerabilidad en la interfaz de mensajería de la aplicación Cisco Webex que podría permitir que un atacante remoto no autenticado modifique enlaces u otro contenido y realice ataques de phishing.

Esta vulnerabilidad existe porque el software afectado no maneja correctamente la representación de caracteres, un atacante podría explotar esta vulnerabilidad enviando mensajes dentro de la interfaz de la aplicación.

Remediación / Referencias

Se recomienda parchear los productos a la última actualización disponible en el Security Center de Cisco.

Por mayor información acceder a:
https://tools.cisco.com/security/center/publicationListing.x

Conclusiones

Las organizaciones globalizadas modernas, que se conectan y comparten en un mercado mundial de industria y comercio, están a su vez compitiendo muy fuertemente a todo nivel. Es por eso que la información y su gestión es muy valorada, tanto así que los estados-nación están utilizando todos los medios para controlar y expandir su status quo.
Observamos diariamente todo tipo de ataques que son causados por conflictos sociales y políticos que son llevados a los medios tecnológicos ya que logran enormes impactos.

La seguridad de la información cada vez es más valorada en los países del primer mundo, tanto es así que en la currícula escolar se contemplan estos elementos. El crecimiento para defendernos de la delincuencia y de las falsedades, no solamente conlleva legislatura, técnicos, políticos, academia y toda la sociedad más concientizada y educada en bioseguridad como sucedió con la pandemia de coronavirus y vimos que no estábamos preparados, lo mismo sucede con la ciberseguridad, no estamos preparados para enfrentar una guerra informática.

Preparemos a nuestros equipos para los peores escenarios, de esta forma evitaremos pérdidas en el futuro, trabajemos en ciberseguridad hoy y en base a todas las mejores prácticas de la industria de la ciberseguridad, que conlleva no solamente a las tecnologías, sino que también a las personas y los procesos de trabajo con las que interactuamos.

Volveremos en dos semanas a publicar un nuevo boletín con más actualidad de nuestro ámbito.