GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1223

En alianza con

TD SYNNEX FORTINET

BOLETIN DE CIBERINTELIGENCIA DE AMENAZAS

Bienvenido a su boletín semanal de ciberseguridad generado por Gamma Ingenieros. A través de esta publicación tenemos el propósito de compartir contenidos relevantes para nuestras operaciones y aliados de negocio.

Aquí encontrará información sobre vulnerabilidades, alertas tempranas, noticias del sector, incidentes de ciberseguridad, tecnologías y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABIILIDADES	1	2	
MALWARE	3	1	
BRECHAS DE SEGURIDAD	1	1	1
NOTICIAS DE CIBERSEGURIDAD		1	2
SECTOR GOBIERNO	1		1
SECTOR FINANCIERO	1		

VULNERABILIDADES

Cisco lanza actualizaciones de seguridad para múltiples productos

Cisco ha lanzado actualizaciones de seguridad para abordar nueve vulnerabilidades de impacto alto y nueve de impacto medio para Cisco IOS XE, Cisco IOS, Cisco DNA Center y otros productos. Los avisos de gravedad alta incluyen vulnerabilidades que, si se explotan, podrían conducir a la ejecución de comandos arbitrarios, aumento de privilegios o denegación de servicio . Un atacante ya autenticado podría explotar algunas de estas vulnerabilidades para tomar el control de un sistema.

Prioridad: 1 Crítico.

Ampliar información:

- https://digital.nhs.uk/cyber-alerts/2023/cc-4289
- https://sec.cloudapps.cisco.com/security/center/publicationListing.x
- https://www.cisa.gov/news-events/alerts/2023/03/23/cisco-releases-security-advisories-multiple-products

---

Vulnerabilidad de apache tomcat revela cookies de sesión a atacantes

Se ha determinado que las versiones 8.5.85/9.0.71/10.1.5/11.0.0-M2 inclusive de Apache Tomcat, tienen una vulnerabilidad que se ha calificado como problemática (software de servidor de aplicaciones). Una característica no identificada del componente conocido como RemoteIpFilter Handler, está rota como resultado de este error. La manipulación con una entrada desconocida da como resultado una vulnerabilidad que implica la transmisión no segura de credenciales.

Prioridad: 2 Urgente.

Ampliar información:

- https://noticiasseguridad.com/vulnerabilidades/vulnerabilidad-de-apache-tomcat-revela-las-cookies-de-sesion-de-aplicacion-a-los-atacantes/
- https://tomcat.apache.org/security-11.html

Del ransomware al ciberespionaje: 55 vulnerabilidades de día cero atacadas en 2022

Hasta 55 vulnerabilidades de día cero fueron explotadas en 2022, con la mayoría de los defectos descubiertos en el software de Microsoft, Google y Apple.

Aunque esta cifra representa una disminución con respecto al año anterior, cuando se aprovecharon 81 vulnerabilidades de día cero, sigue representando un aumento significativo en los últimos años de los actores de amenazas los cuales, aprovechan fallos de seguridad desconocidos en su beneficio.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.ciberseguridadlatam.com/2023/03/22/del-ransomware-al-ciberespionaje-55-vulnerabilidades-de-dia-cero-atacadas-en-2022/

Recomendaciones generales sobre vulnerabilidades:

- Mantener los sistemas operativos y/o aplicaciones actualizadas.
- Realizar actualizaciones directamente desde fabricantes y/o desarrolladores oficiales.
- Emplear controles compensatorios si no se puede realizar la actualización inmediatamente, dichos controles pueden incluir controles tecnológicos y soluciones de seguridad avanzadas que le permitan minimizar el riesgo de que alguna vulnerabilidad sea explotada.
- Tener una política y un plan de mitigación de vulnerabilidades periódico.
- Contar con soluciones de gestión de vulnerabilidades que le permita hacer la priorización de estas.
- Adquirir tecnologías que le permitan bloquear accesos mal intencionados o intentos de explotación de vulnerabilidades conocidas y de día cero.
- Contar con servicios de Ethical Hacking para identificar posibles superficies de ciberataque antes de que lo hagan sus adversarios, protegiendo los datos sensibles de un uso indebido o de robo, ayudando a prevenir las amenazas en la seguridad de los datos e identificar las vulnerabilidades que pueden ir más allá del sistema perimetral, con el fin de establecer un análisis holístico de las amenazas que puedan comprometer la seguridad de los datos críticos de la compañía, entre otras.

MALWARE

El malware Emotet se distribuye ahora en archivos de Microsoft OneNote

El malware Emotet, roba los contactos y contenido de los correos electrónicos una vez cargados para utilizarlos en futuras campañas de spam. Además, descarga otras cargas útiles que proporcionan acceso inicial a la red corporativa. Lo cual, les permite llevar a cabo ciberataques contra la empresa, incluyendo ataques de ransomware, robo de datos, ciberespionaje y extorsión.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.ciberseguridadlatam.com/2023/03/21/el-malware-emotet-se-distribuye-ahora-en-archivos-de-microsoft-onenote/

AndroxGh0st malware utilizado activamente

FortiGuard Labs es consciente de que el malware AndroxGh0st se usa activamente en el campo para apuntar principalmente a archivos ".env" que contienen información confidencial para varias aplicaciones de alto perfil, como AWS, O365, SendGrid y Twilio del marco de aplicaciones web de Laravel.

Prioridad: 2 Urgente.

Ampliar información:

- https://fortiguard.fortinet.com/threat-signal-report/5066

Falso correo en nombre de la Registraduría Nacional de la República de Colombia contiene malware

En los últimos años hemos visto varias campañas de phishing dirigidas a Colombia y otros países de la región intentando distribuir malware. Es común que los nombres de los organismos públicos sean utilizados por los atacantes para intentar convencer a las personas y obtener así sus datos.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.welivesecurity.com/la-es/2023/03/21/phishing-nombre-registraduria-nacional-republica-colombia-malware/

Tres nuevas técnicas de ocultación del malware FakeCalls

Los desarrolladores del software malicioso conocido como FakeCalls, diseñado para dispositivos Android, han creado tres nuevas técnicas para ocultarlo en el sistema y evitar que las herramientas de seguridad lo detecten. Este software malicioso se distribuye a través de aplicaciones bancarias falsas.

Prioridad: 1 Crítico.

Ampliar información:

- https://cybersecuritynews.es/tres-nuevas-tecnicas-de-ocultacion-del-malware-fakecalls/

Recomendaciones generales sobre Malware:

- Controlar de forma minuciosa las conexiones de acceso remoto a su infraestructura: prohíba las conexiones desde redes públicas, permita el acceso RDP solo mediante un canal VPN y use contraseñas seguras y únicas con la autenticación en dos pasos.

- Mantener actualizado el software crítico de manera oportuna, poniendo énfasis en el sistema operativo, las soluciones de seguridad, los clientes de VPN y las herramientas de acceso remoto.
- Mantener a sus empleados constantemente en capacitaciones de concientización de ciberseguridad y en programas de sensibilización de ciberseguridad. En Gamma Ingenieros contamos con un programa completo de sensibilización en ciberseguridad, para obtener más información contacte a su gerente de cuenta, preguntando por nuestro programa de sensibilización y nuestra plataforma propietaria, Gamma Cyberacademy ©.
- Emplear soluciones de ciberseguridad avanzadas para proteger los dispositivos de trabajo y el perímetro de la red corporativa.
- Mantener actualizadas sus soluciones de ciberseguridad.
- Descargar aplicaciones solo de fuentes de confianza, como la tienda oficial de aplicaciones de Google Play Store.
- Revisar las calificaciones y opiniones de otras personas antes de descargar cualquier aplicación, especialmente si es una aplicación bancaria o financiera.
- No responder a llamadas telefónicas de números desconocidos o sospechosos, especialmente si solicitan información personal o financiera.
- No compartir información personal o financiera a través del teléfono o correo electrónico, a menos que esté seguro de la identidad del destinatario.

BRECHAS DE SEGURIDAD

Telepizza, víctima de un ataque de ransomware del Grupo ruso LockBit

Telepizza parece haber sido el último objetivo de un ataque informático, donde los sistemas internos de la empresa podrían haberse visto comprometidos.

Prioridad: 3 Importante.

Ampliar información:

- https://tugatech.com.pt/t52465-telepizza-e-alvo-de-ataque-de-ransomware
- https://blog.elhacker.net/2023/03/telepizza-victima-del-ransomware-ruso-lockbit.html

---

Hitachi Energy confirma una violación de datos, tras los ataques de Cl0p GoAnywhere

Hitachi Energy confirmó que sufrió una violación de datos después de que la banda de ransomware Cl0p robara datos utilizando una vulnerabilidad de día cero GoAnyway.

Algunas empresas colombianas también están incluidas en el listado de la banda de ransomware Cl0p.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.ciberseguridadlatam.com/2023/03/20/hitachi-energy-confirma-una-violacion-de-datos-tras-los-ataques-de-clop-goanywhere/
- https://www.bleepingcomputer.com/news/security/hitachi-energy-confirms-data-breach-after-clop-goanywhere-attacks/

Ferrari confirma que fue víctima de un ataque de ransomware

La firma del Cavallino Rampante fue víctima de un nuevo ciberataque a través de ransomware o secuestro de datos. La compañía ha enviado una misiva a sus clientes informando de los detalles y explicando que algunos datos sensibles como nombre, apellidos, dirección postal, correo electrónico o teléfono móvil de los clientes se han visto expuestos.

COMUNICACIÓN PARA LOS CLIENTES

Estimado/a Ferrarista:

Lamentamos informarle de que en Ferrari hemos sufrido un incidente durante el cual unos ciberdelincuentes han podido acceder a un número limitado de sistemas de nuestro entorno de TI. Como parte de este incidente, se han visto expuestos algunos datos relativos a nuestros clientes, entre ellos nombre, dirección postal, dirección de correo electrónico y número de teléfono. Es posible que sus datos estén incluidos. Sin embargo, según nuestras investigaciones, no se han robado datos de pago, números de cuenta corriente ni otra información confidencial de cobro, así como tampoco detalles de compras o pedidos de coches de Ferrari.

Prioridad: 2 Urgente.

Ampliar información:

- https://blog.elhacker.net/2023/03/ferrari-confirma-que-fue-victima-de-un-ataque-de-ransomware-con-robo-datos-personales-clientes.html
- https://www.adslzone.net/noticias/seguridad/ferrari-ciberataque-ransomware/
- https://blog.segu-info.com.ar/2023/03/ferrari-afectado-por-un-ransomware.html
- https://www.gpfans.com/en/f1-news/103964/ferrari-hacked-customers-ransomware-data-attack/

NOTICIAS DE CIBERSEGURIDAD

Clonación vocal a través de inteligencia artificial: la nueva herramienta para estafar

El nuevo programa de 'Horizonte' ha abordado uno de los nuevos métodos que se están utilizando hoy en día para estafar: la inteligencia artificial permite recrear voces. Chema Alonso, hacker, ha estado presente en plató para revela todos los detalles de esta nueva técnica.

Prioridad: 3 Importante.

Ampliar información:

- https://www.cuatro.com/horizonte/20230323/peligros-clonacion-vocal-inteligencia-artificial-estafas_18_09084182.html

---

Cajeros automáticos de Bitcoin de General Bytes, hackeados para robar fondos

Uno de los principales proveedores de cajeros automáticos de Bitcoin insta a sus clientes a actualizar sus sistemas inmediatamente después de revelar que unos piratas informáticos

explotaron una vulnerabilidad de día cero en su software el pasado fin de semana para robar fondos.

Prioridad: 3 Importante.

Ampliar información:

- https://www.ciberseguridadlatam.com/2023/03/22/cajeros-automaticos-de-bitcoin-de-general-bytes-hackeados-para-robar-fondos/
- https://www.bleepingcomputer.com/news/security/general-bytes-bitcoin-atms-hacked-using-zero-day-15m-stolen/
- https://www.elespanol.com/omicrono/software/20230321/robo-millonario-bitcoins-logrado-hackear-cajeros-criptomonedas/750174992_0.html

---

Crecen en un 57% los ciberataques a niños a través de videojuegos

Los expertos de Kaspersky detectaron más de siete millones de ciberataques a niños a través de videojuegos durante 2022. El informe "The dark side of kids virtual gaming worlds" revela que los ciberataques a los gamers de menor edad se incrementaron un 57% el año pasado. Los ciberdelincuentes se sirven de páginas de phishing que imitan videojuegos como Roblox, Minecraft, Fortnite o Apex Legends para acceder a los dispositivos de sus padres mediante la descarga de software malicioso.

Prioridad: 2 Urgente.

Ampliar información:

- https://cybersecuritynews.es/crecen-un-57-los-ciberataques-a-ninos-a-traves-de-videojuegos/
- https://www.kaspersky.com/blog/threats-in-kids-gaming-worlds/