GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1623

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	5		
MALWARE	2	3	
BRECHAS DE SEGURIDAD		1	1
NOTICIAS DE CIBERSEGURIDAD		1	1

VULNERABILIDADES

Cisco publica avisos de seguridad para varios productos

Cisco ha publicado actualizaciones de seguridad para vulnerabilidades que afectan a Industrial Network Director (IND), Modeling Labs, StarOS Software y BroadbandWorks Network Server. Un atacante remoto podría explotar algunas de estas vulnerabilidades para tomar el control de un sistema afectado.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.cisa.gov/news-events/alerts/2023/04/21/cisco-releases-security-advisories-multiple-products
- https://sec.cloudapps.cisco.com/security/center/publicationListing.x

---

Vulnerabilidades de ThinkPHP RCE (CVE-2019-9082, CVE-2018-20062) explotadas activamente

FortiGuard Labs está observando la explotación activa de varias vulnerabilidades de ejecución remota de código de ThinkPHP (CVE-2019-9082 y CVE-2018-20062). La explotación exitosa de las vulnerabilidades podría permitir que un atacante remoto ejecute código arbitrario en el sistema afectado. Ambas vulnerabilidades están en el catálogo de Vulnerabilidades Explotadas Conocidas (KEV) de CIS.

Prioridad: 1 Crítico.

Ampliar información:

- https://fortiguard.fortinet.com/threat-signal-report/5142

Google Chrome con vulnerabilidades nuevas

La actualización 112.0.5615.137 para Chrome corrige ocho fallas de seguridad, incluida al menos una que puede haber sido aprovechada activamente. Esta vulnerabilidad (CVE-2023-2136) se describe como un desbordamiento de enteros en la librería multiplataforma de gráficos 2D Skia y aparece como un error de alto riesgo. Como siempre, Google no revela cómo se solucionó la falla.

Prioridad: 1 Crítico.

Ampliar información:

- https://blog.segu-info.com.ar/2023/04/otro-zero-day-en-chrome-parchea.html
- https://sites.google.com/a/chromium.org/dev/Home/chromium-security

---

Importante Actualización de iOS y macOS de Apple

Se han vuelto a detectar un par de vulnerabilidades graves en los sistemas operativos de Apple. Por ello, es importante actualizar a iOS 16.4.1 y macOS 13.3.1. Se debe tener en cuenta que las actualizaciones también están disponibles para iOS 15 y macOS 11 y 12.

Prioridad: 1 Crítico.

Ampliar información:

- https://latam.kaspersky.com/blog/ios-macos-vulnerabilities-april-2023/26214/

Oracle lanza actualizaciones de seguridad

Oracle ha publicado su aviso de actualización a parches críticos, el boletín de terceros de Solaris y el boletín de Linux a abril de 2023 con el fin de abordar las vulnerabilidades que afectan a varios productos. Un atacante remoto podría explotar algunas de estas vulnerabilidades para tomar el control de un sistema afectado.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.cisa.gov/news-events/alerts/2023/04/21/oracle-releases-security-updates

---

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 ransomware afiliado ALPHV/BlackCat ataca los fallos de la solución Veritas Backup

Un afiliado de la banda de ransomware ALPHV/BlackCat, rastreado como UNC4466, fue observado explotando tres vulnerabilidades en la solución Veritas Backup para obtener acceso inicial a la red objetivo.

A diferencia de otros afiliados de ALPHV, UNC4466 no se basa en credenciales robadas para el acceso inicial a los entornos de las víctimas. Los investigadores de Mandiant observaron por primera vez a esta filial atacando problemas de Veritas el 22 de octubre de 2022.

Prioridad: 1 Crítico.

Ampliar información:

- https://securityaffairs.com/144438/cyber-crime/alphv-blackcat-ransomware-veritas-flaws.html
- https://blog.segu-info.com.ar/2023/04/el-ransomware-afiliado-alphvblackcat.html
- https://blog.elhacker.net/2023/04/afiliado-del-grupo-ransomware-blackcat-atacando-veritas-backup.html

Videos de YouTube distribuyen el malware Aurora Stealer

Investigadores de ciberseguridad han detallado el funcionamiento interno de un cargador altamente evasivo llamado "in2al5d p3in4er" (léase: impresora no válida) que se utiliza para distribuir el malware Aurora para el robo de información.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.ciberseguridadlatam.com/2023/04/21/videos-de-youtube-que-distribuyen-el-malware-aurora-stealer-a-traves-de-un-cargador-muy-evasivo/

Operación Guinea Pig: campaña que intenta distribuir el malware AgentTesla en México y otros países de América Latina

Investigadores de seguridad analizaron una campaña que intenta distribuir el malware AgentTesla apuntando principalmente a México, Colombia y Ecuador mediante correos de phishing especialmente dirigidos.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.welivesecurity.com/la-es/2023/04/20/operacion-guinea-pig-correos-phishing-malware-agenttesla-mexico-america-latina/

Las víctimas de ransomware alcanzan su máximo histórico, con un aumento del 91% en marzo

El equipo de Global Threat Intelligence de NCC Group registra un aumento sin precedentes en el número de ataques de ransomware en marzo, llegando a los 459. Esto supone un 91% más que en febrero.

La red delictiva Cl0p fue la más activa, llegando a las 129 víctimas registradas.
Los sectores más afectados fueron el industrial (32 %), el de consumo cíclico (13 %) y el tecnológico (12 %).

Prioridad: 2 Urgente.

Ampliar información:

- https://cybersecuritynews.es/las-victimas-de-ransomware-alcanzan-su-maximo-historico-con-un-aumento-del-91-en-marzo/

Los Mac de Apple han escapado durante mucho tiempo al ransomware. Eso podría estar cambiando.

El descubrimiento de encriptadores maliciosos para ordenadores Apple podría anunciar nuevos riesgos para los usuarios de macOS si el malware sigue evolucionando.

Prioridad: 2 Urgente.

Ampliar información:

- https://blog.segu-info.com.ar/2023/04/el-ransomware-lockbit-confirma-que.html
- https://thehackernews.com/2023/04/lockbit-ransomware-now-targeting-apple.html
- https://www.ciberseguridadlatam.com/2023/04/18/los-mac-de-apple-han-escapado-durante-mucho-tiempo-al-ransomware-eso-podria-estar-cambiando/

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

Grupo de gamers expuso una de las filtraciones más graves de Estados Unidos

Estados Unidos enfrenta una de las mayores filtraciones de datos. Hay quienes ya lo han comparado con el caso *>WikiLeaks*, que sacudió al mundo en 2010. Y aunque sus dimensiones —por ahora— no se comparan con los más de 250 mil documentos secretos publicados entonces, la Casa Blanca ha admitido la relevancia de esta nueva fuga. Según el Pentágono, representa un "riesgo muy grave para la seguridad nacional".

Prioridad: 3 Importante.

Ampliar información:

- https://hipertextual.com/2023/04/gamers-filtracion-estados-unidos

---

Grupo Nutresa denunció posible ataque de ‘ransomware’ a sus sistemas

El Grupo Nutresa, empresa líder en alimentos de Colombia, informó que ha identificado un evento de posible ransomware en sus sistemas informáticos. Según el comunicado emitido por la compañía, hasta el momento no se ha evidenciado un compromiso a la

integridad de los datos de la Ooganización ni de la información de sus clientes, proveedores, consumidores y demás grupos relacionados.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.bluradio.com/blu360/antioquia/nutresa-confirmo-que-esta-siendo-victima-de-un-ciberataque-de-ransomware-rg10
- https://www.semana.com/economia/empresas/articulo/grupo-nutresa-denuncio-posible-ataque-de-ransomware-a-sus-sistemas/202320/

NOTICIAS DE CIBERSEGURIDAD

Facebook pagará una multa millonaria a usuarios en EE.UU. por Cambridge Analytica

Facebook tendrá que pagar una multa millonaria por el escándalo de privacidad con Cambridge Analytica. Una demanda colectiva organizada por usuarios de la red social ha llegado a buen puerto, porque la red social va a tener que pagar unos 725 millones de dólares. Una cantidad que se va a repartir entre los usuarios en el país.

Prioridad: 3 Importante.

Ampliar información:

- https://hipertextual.com/2023/04/facebook-multa-cambridge-analytica-usuarios-ee-uu

Servidores SQL de Microsoft pirateados para desplegar el ransomware Trigona

Atacantes están pirateando servidores Microsoft SQL (MS-SQL) mal protegidos y expuestos a Internet para desplegar cargas útiles del ransomware Trigona y cifrar todos los archivos.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/microsoft-sql-servers-hacked-to-deploy-trigona-ransomware/