@mindefarg
argentina.gob.ar/defensa
Ministerio de Defensa
Argentina
Edificio Libertador
Azopardo 250 (CABA)
(54 11) 4346-8836/9

Subsecretaría de Ciberdefensa

Boletín de Noticias de Ciberseguridad

Informe sobre incidentes y ciberamenazas Nro. 129 – Año 2021

Este boletín periódico es un resumen seleccionado de las últimas vulnerabilidades, incidentes de seguridad e informes recopilados de fuentes internacionales conocidas dedicadas a la seguridad informática. Está destinado a las áreas de ciberseguridad de la Defensa como información de interés general para su difusión.

31/08/21

- Se ha filtrado información, pasaporte y datos sanitarios, de la aplicación indonesia COVID-19 de análisis y rastreo para viajeros.
  https://www.zdnet.com/article/passport-info-and-healthcare-data-leaked-from-indonesias-covid-19-test-and-trace-app-for-travellers/
- Bangkok Airways admite que atacantes robaron datos de los pasajeros.
  https://www.infosecurity-magazine.com/news/bangkok-airlines-attackers-stole/
  https://securityaffairs.co/wordpress/121702/data-breach/lockbit-gang-bangkok-airways.html
- Intrusos de Accellion expusieron los datos de los pacientes de un importante sistema hospitalario de Michigan.
  https://www.cyberscoop.com/accellion-breach-exposed-data-from-patients-at-major-michigan-hospital-system/

01/09/21

- **La plataforma Cream Finance sufrió un robo de más de 34 millones de dólares en criptodivisas.**
  https://www.zdnet.com/article/cream-finance-wallet-pilfered-for-34-million-in-cryptocurrency/
- Un empleado despedido de una cooperativa de crédito de Nueva York destruye 21 GB de datos como venganza.
  https://www.bleepingcomputer.com/news/security/fired-ny-credit-union-employee-nukes-21gb-of-data-in-revenge/

02/09/21

- Autodesk revela que fue blanco de los hackers rusos de SolarWinds.
  https://www.cyberscoop.com/solarwinds-autodesk-hack-russia-us/
- Una empresa de VoIP británica recibe una "colosal petición de rescate"
  https://www.theregister.com/2021/09/02/uk_voip_telcos_revil_ransom/

TRABAJOS, ESTUDIOS Y ANÁLISIS ABOCADOS A LAS TEMÁTICAS DE LA CIBERSEGURIDAD

- La vulnerabilidad de ProxyToken afecta al programa de la Iniciativa del Día Cero.
  https://exchange.xforce.ibmcloud.com/collection/8f5fd9500bd69d22653ed16a334fca15
  https://therecord.media/proxytoken-vulnerability-can-modify-exchange-server-configs/
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-33766
- **Más detalles de la desclasificación de criptoanálisis militar de la NSA.**
  https://www.schneier.com/blog/archives/2021/08/more-military-cryptanalytics-part-iii.html
- Ataque de phishing utiliza un truco furtivo para robar tus contraseñas, advierte Microsoft.
  https://www.zdnet.com/article/this-phishing-attack-is-using-a-sneaky-trick-to-steal-your-passwords-warns-microsoft/

- **Lista de filtraciones de datos y ciberataques en agosto de 2021.**
https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-august-2021-61-million-records-breached
- Los errores de BrakTooth ponen en riesgo a millones de dispositivos con Bluetooth.
https://thehackernews.com/2021/09/new-braktooth-flaws-leave-millions-of.html
- El inicio de sesión en Google Play permiten el monitoreo encubierto de la ubicación.
https://threatpost.com/google-play-covert-location-tracking/169151/

NOTAS DE INTERÉS

- Coinbase informó erróneamente de los cambios de 2FA a 125.000 clientes.
https://arstechnica.com/information-technology/2021/08/coinbase-erroneously-reported-2fa-changes-to-125000-customers/
- CISA añade la autenticación de factor único a la lista de malas prácticas.
https://thehackernews.com/2021/08/cisa-adds-single-factor-authentication.html.
- Los piratas utilizan WebSVN para desplegar el nuevo malware Mirai.
https://www.itpro.co.uk/security/malware/360731/hackers-use-websvn-to-deploy-new-mirai-variant-malware
- investigadores proponen un esquema de autenticación Bluetooth basado en el aprendizaje automático.
https://thehackernews.com/2021/08/researchers-propose-machine-learning.html
- La alarma Fortress de seguridad doméstica se puede desarmar a distancia.
https://threatpost.com/fortress-home-security-remote-disarmament/169069/
https://securityaffairs.co/wordpress/121679/hacking/fortress-s03-home-security-system-flaws.html
- Estafadores están reclutando a personas de habla inglesa para campañas de ataque de correo electrónico comercial.
https://www.zdnet.com/article/scam-artists-are-recruiting-english-speakers-for-business-email-campaigns/
- “No utilice la autenticación de factor único en los sistemas expuestos a Internet”, advierte CISA.
https://www.ehackingnews.com/2021/09/do-not-use-single-factor-authentication.html
- El mercado de análisis de tráfico de red alcanzará los 5.690 millones de dólares en 2028.
https://www.helpnetsecurity.com/2021/09/02/network-traffic-analysis-market-2028/

ACTUALIZACIONES DE SEGURIDAD

- Twitter añade el modo de seguridad para bloquear automáticamente el acoso en línea.
https://www.zdnet.com/article/twitter-creates-safety-mode-to-temporarily-block-accounts-caught-insulting-users/
- Publicación de la actualización acumulativa de Windows 10 KB5005101 con 34 correcciones.
https://www.bleepingcomputer.com/news/microsoft/windows-10-kb5005101-cumulative-update-released-with-34-fixes/
- Google difunde actualizaciones de seguridad para Chrome.
https://us-cert.cisa.gov/ncas/current-activity/2021/09/01/google-releases-security-updates-chrome
- Cisco corrige un fallo crítico de derivación de autenticación con un *exploit* público.
https://www.bleepingcomputer.com/news/security/cisco-fixes-critical-authentication-bypass-bug-with-public-exploit/