@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. 127 – 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.

17/08/2021

- El banco Chase filtró accidentalmente información de clientes a otros clientes.
https://www.bleepingcomputer.com/news/security/chase-bank-accidentally-leaked-customer-info-to-other-customers/
- **El gobierno brasileño informa del ataque del ransomware al Tesoro Nacional.**
https://www.bleepingcomputer.com/news/security/brazilian-government-discloses-national-treasury-ransomware-attack/
- La aseguradora japonesa Tokio Marine es la última víctima del ransomware.
https://www.cyberscoop.com/tokio-marine-ryan-specialty-group-ransomware-cyber-insurance/
- Filtración de datos de rastreo de contactos en el estado de Indiana, EE.UU.
https://www.infosecurity-magazine.com/news/indiana-contact-tracing-data/

18/08/2021

- Piratas informáticos de Corea del Norte instalan *exploits* de navegador en sitios de Corea del Sur para propagar malware.
https://thehackernews.com/2021/08/nk-hackers-deploy-browser-exploit-on.html
- El propietario de un servicio de *blanqueo* de criptomonedas en la web oscura, conocido como Helix, se ha declarado culpable de lavar más de 300 millones de dólares en bitcoins.
https://www.bleepingcomputer.com/news/security/bitcoin-mixer-owner-pleads-guilty-to-laundering-over-300-million/

19/08/2021

- La bolsa de criptomonedas Liquid pierde 94 millones de dólares tras el hackeo.
https://www.cnbc.com/2021/08/19/liquid-cryptocurrency-exchange-hack.html
- Los “actores de la amenaza” *hackearon* la Oficina del Censo de Estados Unidos en 2020 aprovechando un error de Citrix.
https://securityaffairs.co/wordpress/121270/reports/us-census-bureau-citrix-flaw.html

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

- Un fallo crítico permite comprometer y controlar de forma remota millones de dispositivos IoT.
https://www.helpnetsecurity.com/2021/08/17/cve-2021-28372/
https://thehackernews.com/2021/08/critical-throughtek-sdk-bug-could-let.html
- Vulnerabilidad BadAlloc que afecta a BlackBerry QNX RTOS.
https://us-cert.cisa.gov/ncas/alerts/aa21-229a
https://www.cyberscoop.com/blackberry-badalloc-medical-vulnerability/
- Aumentan las vulnerabilidades de los sistemas de control integrado (ICS) a medida que se incrementan los ataques.

https://betanews.com/2021/08/18/ics-vulnerabilities-rise-attacks-increase/

- Falsas aplicaciones de criptominería inundan Google Play.
https://threatpost.com/bogus-cryptomining-apps-google-play/168785/
- **CISA comparte una guía sobre cómo prevenir las violaciones de datos por ransomware.**
https://www.bleepingcomputer.com/news/security/cisa-shares-guidance-on-how-to-prevent-ransomware-data-breaches/
- Error de EoP (elevation of privilege) de Windows detallado por Google Project Zero.
https://threatpost.com/windows-eop-bug-detailed-by-google-project-zero/168823/

NOTAS DE INTERÉS

- Mastercard anuncia el fin de la banda magnética en las tarjetas de pago.
https://www.zdnet.com/article/mastercard-waves-goodbye-to-the-magnetic-stripe-on-payment-cards/
- Apple: La puerta trasera de detección de imágenes CSAM tiene un alcance "limitado".
https://threatpost.com/apple-image-detection-backdoor/168727/
- Colonial Pipeline admite supuestamente una filtración de datos del ataque de mayo pasado.
https://www.infosecurity-magazine.com/news/colonial-pipeline-admits-data/
- El ransomware LockBit 2.0 se extiende por todo el mundo.
https://threatpost.com/lockbit-ransomware-proliferates-globally/168746/
- El malware HolesWarm se aprovecha de los servidores Windows y Linux sin parches.
https://threatpost.com/holeswarm-malware-windows-linux/168759/
- Equipo de riesgos informáticos descubre una vulnerabilidad previamente desconocida en el software de Autodesk durante una prueba de penetración en un cliente.
https://www.tripwire.com/state-of-security/security-data-protection/risk-team-discovers-unknown-vulnerability-autodesk-software/
- **GitHub empuja a los usuarios a activar el 2FA tras el fin de la autenticación por contraseña para las operaciones de Git.**
https://www.zdnet.com/article/github-pushes-users-to-enable-2fa-following-end-of-password-authentication-for-git-operations/
- Cisco no corregirá la vulnerabilidad RCE de día cero en los routers VPN al final de su vida útil.
https://www.bleepingcomputer.com/news/security/cisco-won-t-fix-zero-day-rce-vulnerability-in-end-of-life-vpn-routers/
- Los investigadores encuentran nuevas pruebas que relacionan el ransomware Diavol con la banda TrickBot.
https://thehackernews.com/2021/08/researchers-find-new-evidence-linking.html

ACTUALIZACIONES DE SEGURIDAD

- Fortinet retrasa el arreglo de un “día cero” que permitía tomar control de servidores remotos.
https://threatpost.com/unpatched-fortinet-bug-firewall-takeovers/168764/
- Ubuntu Linux obtiene la certificación para cargas de trabajo seguras y reguladas.
https://betanews.com/2021/08/17/ubuntu-certified-for-secure-regulated-workloads/
- Adobe resuelve dos vulnerabilidades críticas en Photoshop.
https://securityaffairs.co/wordpress/121238/security/adobe-fixes-critical-photoshop-flaws.html