@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. 97/2021

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.

04/04/2021

- Un controlador vulnerable de Dell pone en peligro cientos de millones de sistemas.
https://threatpost.com/dell-kernel-privilege-bugs/165843/
- Tres nuevas familias de malware se encontraron en una campaña de phishing financiero global.
https://www.zdnet.com/article/researchers-find-three-new-malware-families-used-in-global-finance-phishing-campaign/
- Millones de PCs de Dell tienen cinco vulnerabilidades, no detectadas durante casi una docena de años, en el código de los controladores de Windows.
https://www.theregister.com/2021/05/04/dell_driver_flaw/
https://www.darkreading.com/threat-intelligence/hundreds-of-millions-of-dell-computers-potentially-vulnerable-to-attack/d/d-id/1340910

05/05/2021

- Nuevos defectos de “21Nails Exim” exponen a millones de servidores de e-mail al pirateo.
https://thehackernews.com/2021/05/alert-new-21nails-exim-bugs-expose.html
- Un masivo ataque de DDoS dejó fuera de servicio a grandes sectores de Internet de Bélgica.
https://www.zdnet.com/article/this-massive-ddos-attack-took-large-sections-of-a-countrys-internet-offline/
- El FBI cierra un falso sitio web destinado a fraudes con la vacuna para el COVID-19.
https://threatpost.com/feds-fake-covid-19-vaccine-phishing-website/165872/

06/05/2021

- Una vulnerabilidad de Qualcomm afecta a casi el 40% de los teléfonos móviles.
https://thehackernews.com/2021/05/new-qualcomm-chip-bug-could-let-hackers.html
- El ransomware Ryuk se introduce en un instituto de investigación biológica a través de un estudiante que no quiso pagar por el software.
https://www.zdnet.com/article/ryuk-ransomware-finds-foothold-in-bio-research-institute-through-a-student-who-wouldnt-pay-for-software/
- La intrusión de datos en CaptureRx afecta a los proveedores de servicios sanitarios.
https://www.infosecurity-magazine.com/news/capturerx-data-breach-impacts/

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

- El nuevo malware "Pingback" de Windows utiliza ICMP para una comunicación encubierta.
https://www.bleepingcomputer.com/news/security/new-windows-pingback-malware-uses-icmp-for-covert-communication/
- APT en acción: XDSpy y Sandworm.
https://cybernews.com/security/apt-in-action-xdspy-and-sandworm/

- Un nuevo bug del TsuNAME DNS permite a los atacantes realizar ataques DDoS.
https://www.bleepingcomputer.com/news/security/new-tsuname-dns-bug-allows-attackers-to-ddos-authoritative-dns-servers/

NOTAS DE INTERÉS

- El Departamento de Defensa de EE.UU. amplía el programa de divulgación de fallos a todos los sistemas de acceso público.
https://www.bleepingcomputer.com/news/security/dod-expands-bug-disclosure-program-to-all-publicly-accessible-systems/
- Facebook prohíbe el intento de Signal de realizar una campaña publicitaria transparente en Instagram.
https://www.zdnet.com/article/facebook-bans-signals-attempt-to-run-transparent-instagram-ad-campaign/
- "Panda Stealer" aparece en archivos de Excel y se propaga a través de Discord para robar criptomonedas de los usuarios.
https://www.zdnet.com/article/panda-stealer-dropped-in-discord-to-steal-user-cryptocurrency/
- Microsoft eliminará pronto el Flash Player de los dispositivos Windows 10.
https://www.welivesecurity.com/2021/05/04/microsoft-remove-flash-player-windows10-devices/
- Los bugs de Cisco permiten crear cuentas de administrador, ejecutando comandos como root.
https://www.bleepingcomputer.com/news/security/cisco-bugs-allow-creating-admin-accounts-executing-commands-as-root/
https://threatpost.com/critical-cisco-sd-wan-hyperflex-bugs/165923/
- Millones de routers de banda ancha antiguos presentan fallas de seguridad.
https://www.zdnet.com/article/millions-of-older-broadband-routers-have-these-security-flaws-warn-researchers/

ACTUALIZACIONES DE SEGURIDAD

- Apple emite parches de seguridad urgentes para errores de día cero que están bajo ataques.
https://thehackernews.com/2021/05/apple-releases-urgent-security-patches.html
https://nakedsecurity.sophos.com/2021/05/04/apple-products-hit-by-fourfecta-of-zero-day-exploits-patch-now/
- Dell publica una actualización de seguridad crítica para corregir graves fallas en los controladores de cientos de millones de sistemas.
https://betanews.com/2021/05/05/dell-issues-critical-security-update-to-patch-serious-driver-flaws-in-hundreds-of-millions-of-systems/
https://www.dell.com/support/kbdoc/es-ar/000186019/dsa-2021-088-dell-client-platform-security-update-for-dell-driver-insufficient-access-control-vulnerability
- VMware corrige un error crítico de RCE en el "vRealize Business for Cloud".
https://www.bleepingcomputer.com/news/security/vmware-fixes-critical-rce-bug-in-vrealize-business-for-cloud/
- IBM ha publicado ocho boletines de seguridad que se aplican a QRadar SIEM.
https://exchange.xforce.ibmcloud.com/collection/a7bb9e91e8aa8ecc0c2e0f4441fec249
- Firefox para Android recibe una actualización crítica para bloquear el problema del robo de cookies.
https://nakedsecurity.sophos.com/2021/05/06/firefox-for-android-gets-critical-update-to-block-cookie-stealing-hole/