@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. 210 – Año 2023

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.

NOTICIAS DE CIBERSEGURIDAD entre el 10/7/23 y el 24/7/23

1. Los investigadores de ciberseguridad descubrieron un nuevo gusano peer-to-peer (P2P) llamado P2PInfect que se dirige a los servidores Redis.
https://securityaffairs.com/148636/malware/p2pinfect-a-rusty-p2p-worm-targets-redis-servers-on-linux-and-windows-systems.html

2. LLM (***Large Languaje Model***) e IA (***Intelligence Artificial***) posicionados para dominar el mundo de AppSec.
https://www.helpnetsecurity.com/2023/07/20/llm-applications-security-risks/

3. Cyber Trust Mark es una etiqueta voluntaria de IoT que se lanzará en 2024. ¿Qué significa?
https://arstechnica.com/information-technology/2023/07/the-cyber-trust-mark-is-a-voluntary-iot-label-coming-in-2024-what-does-it-mean/

4. ChatGPT está creando nuevos riesgos para la seguridad nacional.
https://www.defensenews.com/opinion/2023/07/20/chatgpt-is-creating-new-risks-for-national-security/

5. Investigadores encuentran 'puerta trasera' en radios policiales y militares cifradas.
https://www.vice.com/en/article/4a3n3j/backdoor-in-police-radios-tetra-burst?utm_source=flipboard&utm_content=user%2Fvice

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

1. CISA comparte herramientas gratuitas para ayudar a proteger los datos en la nube.
https://www.bleepingcomputer.com/news/security/cisa-shares-free-tools-to-help-secure-data-in-the-cloud/

2. Microsoft publicó un informe titulado " Análisis de las técnicas Storm-0558 para el acceso no autorizado al correo electrónico".
https://nakedsecurity.sophos.com/2023/07/18/microsoft-hit-by-storm-season-a-tale-of-two-semi-zero-days/

3. Análisis exhaustivo de muestras de ataques iniciales que explotan la vulnerabilidad CVE-2023-23397.
https://securelist.com/analysis-of-attack-samples-exploiting-cve-2023-23397/110202/

4. El grupo de delitos cibernéticos FIN8 está utilizando una versión renovada de la puerta trasera Sardonic para entregar el ransomware BlackCat.
https://securityaffairs.com/148569/cyber-crime/fin8-group-spotted-delivering-the-blackcat-ransomware.html

5. Modelo de Madurez de la Capacidad en Ciberseguridad para las Naciones (CMM) ayuda a los países a comprender lo que funciona, lo que no y por qué, en todos los ámbitos de la capacidad en ciberseguridad
https://gcscc.ox.ac.uk/cmm-2021-edition

NOTAS DE INTERÉS

1. Pekín quiere hacer aún más grande el Gran Firewall de China.
https://www.theregister.com/2023/07/17/great_firewall_even_greater/

2. CISA añade una vulnerabilidad conocida, muy explotada, a su catálogo.
https://www.cisa.gov/news-events/alerts/2023/07/17/cisa-adds-one-known-exploited-vulnerability-catalog

3. Se revela la identidad de un hacker de sombrero negro después infectar su propio ordenador con malware.
https://www.securityweek.com/black-hat-hacker-exposes-real-identity-after-infecting-own-computer-with-malware/

4. Los satélites están plagados de fallas básicas de seguridad.
https://www.wired.com/story/satellites-basic-security-flaws/

5. Cómo proteger y asegurar sus datos de 10 maneras.
https://www.techrepublic.com/article/how-to-protect-and-secure-data/

ACTUALIZACIONES DE SEGURIDAD

1. Vulnerabilidad XSS crítica en Zimbra explotada (CVE-2023-34192).
https://www.helpnetsecurity.com/2023/07/17/cve-2023-34192/

2. Oracle lanza 508 nuevos parches de seguridad con la CPU de julio de 2023.
https://www.securityweek.com/oracle-releases-508-new-security-patches-with-july-2023-cpu/

3. Chrome 115 Parches 20 Vulnerabilidades.
https://www.securityweek.com/chrome-115-patches-20-vulnerabilities/

4. Es probable que aumente la explotación del nuevo Citrix Zero-Day. CVE-2023-3519 .
https://www.securityweek.com/exploitation-of-new-citrix-zero-day-likely-to-increase-organizations-warned/

5. CVE-2023-38408: Ejecución remota de código en el ssh-agent reenviado de OpenSSH.
a) https://blog.qualys.com/vulnerabilities-threat-research/2023/07/19/cve-2023-38408-remote-code-execution-in-opensshs-forwarded-ssh-agent
b) https://thehackernews.com/2023/07/new-openssh-vulnerability-exposes-linux.html

6. CVE-2023-36884: Una mirada detallada a la reciente vulnerabilidad de Microsoft.
https://www.picussecurity.com/resource/blog/cve-2023-36884-a-detailed-look-at-the-recent-microsoft-vulnerability

7. CISA advierte a las agencias gubernamentales que parcheen los servidores de Adobe ColdFusion.
https://www.bleepingcomputer.com/news/security/cisa-warns-govt-agencies-to-patch-adobe-coldfusion-servers/

8. Fortinet advierte sobre falla crítica de RCE en dispositivos FortiOS y FortiProxy. `CVE-2023-33308`.
https://www.bleepingcomputer.com/news/security/fortinet-warns-of-critical-rce-flaw-in-fortios-fortiproxy-devices/