Subsecretaría de Ciberdefensa

Boletín de Noticias de Ciberseguridad

Informe sobre incidentes y ciberamenazas Nro. 208 – 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 7/6/23 y el 23/6/23

1. Fortinet ha publicado varias versiones de FortiOS, el sistema operativo/firmware de sus firewalls Fortigate y otros dispositivos.
https://www.helpnetsecurity.com/2023/06/11/cve-2023-27997/

2. Accenture anuncia una inversión de 3.000 millones de dólares en IA.
https://www.helpnetsecurity.com/2023/06/13/accenture-ai-investment/

3. Un novedoso ataque roba claves de cifrado almacenadas en tarjetas inteligentes y smartphones usando cámaras comerciales, gravando los LED de encendido, a 20 metros de distancia.
https://arstechnica.com/information-technology/2023/06/hackers-can-steal-cryptographic-keys-by-video-recording-connected-power-leds-60-feet-away/

4. Una campaña de ataques tipo "agresores en el medio" afecta a docenas de organizaciones mundiales.
https://thehackernews.com/2023/06/adversary-in-middle-attack-campaign.html

5. Ciberdelincuentes chinos explotan vulnerabilidad Zero-day de VMware en sistemas Windows y Linux
https://unaaldia.hispasec.com/2023/06/ciberdelincuentes-chinos-explotan-vulnerabilidad-zero-day-de-vmware-en-sistemas-windows-y-linux.html

6. ¿Recibiste al azar un reloj inteligente? No lo actives.
https://www.c4isrnet.com/cyber/2023/06/22/randomly-received-a-smartwatch-dont-turn-it-on-investigators-warn/

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

1. Amenazas DDoS y defensa: cómo ciertas hipótesis pueden conducir a un ataque.
https://www.techrepublic.com/article/ddos-threats-defense/

2. Patch Tuesday corrige 4 errores críticos de RCE y un montón de agujeros de Office.
https://nakedsecurity.sophos.com/2023/06/14/patch-tuesday-fixes-4-critical-rce-bugs-and-a-bunch-of-office-holes/

3. Nuevo informe expone el implante de spyware de la Operación Triangulación dirigido a dispositivos iOS.
https://thehackernews.com/2023/06/new-report-exposes-operation.html

4. Defecto crítico 'nOAuth' en Microsoft Azure AD habilita la adquisición completa de cuenta. https://thehackernews.com/2023/06/critical-noauth-flaw-in-microsoft-azure.html

5. Por qué los CISO deberían preocuparse por los ataques basados en el espacio. https://www.csoonline.com/article/3700188/why-cisos-should-be-concerned-about-space-based-attacks.html

NOTAS DE INTERÉS

1. ¿Cómo es posible que algunas empresas se vean comprometidas una y otra vez? https://securityintelligence.com/articles/how-do-some-companies-get-compromised-again-and-again/

2. Gobierno de EEUU sufre un ciberataque masivo: máxima alerta en la Casa Blanca. https://www.ambito.com/mundo/gobierno-eeuu-sufre-un-ciberataque-masivo-maxima-alerta-la-casa-blanca-n5746815

3. Microsoft: Rusia envió a su equipo B a borrar los discos duros ucranianos. https://www.theregister.com/2023/06/16/microsoft_cadet_blizzard_threat/

4. Proteja y administre las extensiones del navegador con Chrome Browser Cloud Management https://security.googleblog.com/2023/06/protect-and-manage-browser-extensions.html

5. Infectan los servidores Linux SSH con el malware Tsunami botnet https://www.bleepingcomputer.com/news/security/hackers-infect-linux-ssh-servers-with-tsunami-botnet-malware/

6. La mayoría de los usuarios ignoran las mejores prácticas de contraseña. https://www.infosecurity-magazine.com/news/users-neglect-best-password/

7. Tres acciones de ciberseguridad que marcan la diferencia. https://www.helpnetsecurity.com/2023/06/19/cybersecurity-programs-improvement/

ACTUALIZACIONES DE SEGURIDAD

1. Vulnerabilidad de VMware Aria ***Operations for Networks*** explotada (CVE-2023-20887). https://www.helpnetsecurity.com/2023/06/21/cve-2023-20887-exploited/

2. ¡Actualizar ahora! ASUS corrige nueve fallas de seguridad https://www.malwarebytes.com/blog/news/2023/06/update-now-asus-fixes-nine-security-flaws

3. Zyxel lanza actualizaciones de seguridad urgentes para vulnerabilidad crítica en dispositivos NAS https://thehackernews.com/2023/06/zyxel-releases-urgent-security-updates.html

4. Solución de problemas de Malwarebytes para Chrome dañado por Windows 11 KB5027231. https://www.bleepingcomputer.com/news/microsoft/malwarebytes-issues-fix-for-chrome-broken-by-windows-11-kb5027231/