BOLETÍN DE CIBERSEGURIDAD

ENERO 2023

ADV

ÍNDICE

NOTICIAS INTERNACIONALES

SYNOLOGY CORRIGE UNA VULNERABILIDAD CRÍTICA

03/01/2023

SYNOLOGY HA ABORDADO UNA VULNERABILIDAD DE GRAVEDAD MÁXIMA QUE AFECTA A LOS SERVIDORES VPN PLUS SERVER.

Synology Inc. (s. f.). Synology_SA_22_26 | Synology Inc. https://www.synology.com/en-us/security/advisory/Synology_SA_22_26

La vulnerabilidad, identificada como CVE-2022-43931 y CVSS de 10.0, puede ser explotada en ataques de baja complejidad sin requerir privilegios en los routers o la interacción del usuario, permitiendo a un atacante remoto la ejecución de comandos arbitrarios.

La compañía ha publicado correcciones para las vulnerabilidades y recomienda a los usuarios actualizar el servidor VPN Plus para SRM a la última versión.

NUEVA CAMPAÑA DE RASPBERRY ROBIN

01/03/2023

INVESTIGADORES DE SECURITY JOES HAN DETECTADO NUEVOS ATAQUES DEL FRAMEWORK RASPBERRY ROBIN CONTRA COMPAÑÍAS DE SEGUROS E INSTITUCIONES FINANCIERAS EN EUROPA.

Joes, S. (2023, 3 enero). Raspberry Robin Detected ITW Targeting Insurance & Financial Institutes In Europe. Security Joes. https://www.securityjoes.com/post/raspberry-robin-detected-itw-targeting-insurance-financial-institutes-in-europe

La actividad de Raspberry Robin fue recientemente documentada también por el equipo de TrendMicro, si bien, los investigadores de Security Joes han podido observar una nueva versión del malware más compleja.

Los ataques recientes documentados en meses anteriores parecen estar orquestados por grupos de piratería que utilizan un marco llamado Raspberry Robin. Este marco automatizado bien diseñado permite a los atacantes las capacidades posteriores a la infección para evadir la detección, moverse lateralmente y aprovechar las infraestructuras de nube confiables de proveedores de alojamiento de datos conocidos como Discord, Azure y Github, entre otros.

os investigadores de amenazas Felipe Duarte, Charles Lomboni y Shlomit Chkool respondieron a incidentes similares dos veces este mes y en cada caso pudieron diseccionar el descargador de su envoltorio principal y revelar el malware que apuntaba al marco Raspberry Robin antes mencionado.

Lo que es único sobre el malware es que está muy ofuscado y es muy complejo de desmontar de forma estática. Retirando dinámicamente una capa a la vez, los investigadores finalmente pudieron encontrar la configuración interna del malware y obtener los indicadores de compromiso (IOC) que contiene. Al leer artículos recientes de TrendMicro y Microsoft , los investigadores pudieron atribuir con éxito el ataque a Raspberry Robin, ya que los IOC se superpusieron con la infraestructura de Raspberry Robin y las tácticas, técnicas y procedimientos (TTP). En ambos ataques, se destacó la misma dirección IP: 85.56.236[.]45 .

MASQUERADS: CAMPAÑA DE DISTRIBUCIÓN DE MALWARE CON GOOGLE ADS

3/01/2023

UNA TÉCNICA RECIÉN DESCUBIERTA PARA ABUSAR DE LA PODEROSA PLATAFORMA PUBLICITARIA DE GOOGLE AD-WORDS ESTÁ DIFUNDIENDO EN MASA RESULTADOS DE BÚSQUEDA PROMOCIONADOS DE FORMA DESHONESTA.

LJoes, S. (2023, 3 enero). Raspberry Robin Detected ITW Targeting Insurance & Financial Institutes In Europe. Security Joes. https://www.securityjoes.com/post/raspberry-robin-detected-itw-targeting-insurance-financial-institutes-in-europe

Señalando sitios de publicidad supuestamente creíbles que están totalmente controlados por actores de amenazas, se utilizan para enmascarar y redirigir a los usuarios que hacen clic en los anuncios a páginas de phishing maliciosas que obtienen la poderosa credibilidad y las capacidades de orientación de los resultados de búsqueda de Google. Al agregar cargas útiles de malware personalizadas, los actores de amenazas están elevando el listón para implementaciones exitosas de malware en PC personales con palabras publicitarias como Grammarly, Malwarebytes y Afterburner, así como con Visual Studio, Zoom, Slack e incluso Dashlane para organizaciones objetivo.

Descubriremos la técnica, mostraremos ejemplos de la vida real y arrojaremos luz sobre uno de los actores de amenazas más grandes titulado " Vermux", aprovechando cantidades masivas de sitios y dominios "masquerAds" servidos principalmente desde Rusia para apuntar a las GPU y Crypto Wallet de los residentes de EE. UU. s: actividades que ya han llamado la atención en el FBI .

MICROSOFT CORRIGE 98 VULNERABILIDADES EN SU PATCH TUESDAY

03/01/2023

LA NUEVA FUNCIÓN HOTPATCHING YA ESTÁ DISPONIBLE DE FORMA GENERAL. CONSULTE LA CARACTERÍSTICA HOTPATCHING PARA MÁQUINAS VIRTUALES (VM) DE WINDOWS SERVER AZURE EDITION PARA OBTENER MÁS INFORMACIÓN

oes, S. (2023, 3 enero). Raspberry Robin Detected ITW Targeting Insurance & Financial Institutes In Europe. Security Joes. https://www.securityjoes.com/post/raspberry-robin-detected-itw-targeting-insurance-financial-institutes-in-europeNoveno

Las actualizaciones de Windows 10 son acumulativas. El lanzamiento de seguridad mensual incluye todas las correcciones de seguridad para las vulnerabilidades que afectan a Windows 10, además de las actualizaciones que no son de seguridad. Las actualizaciones están disponibles a través del Catálogo de actualizaciones de Microsoft . Para obtener información sobre el ciclo de vida y las fechas de soporte para los sistemas operativos Windows 10, consulte la hoja de datos del ciclo de vida de Windows .

Microsoft está mejorando las notas de la versión de Windows. Para obtener más información, consulte Qué sigue para las notas de la versión de Windows .

Puede encontrar una lista de las últimas actualizaciones de la pila de servicio para cada sistema operativo en ADV990001 . Esta lista se actualizará cada vez que se publique una nueva actualización de la pila de servicios. Es importante instalar la última actualización de la pila de servicio .

Además de los cambios de seguridad para las vulnerabilidades, las actualizaciones incluyen actualizaciones de defensa en profundidad para ayudar a mejorar las funciones relacionadas con la seguridad.

Los clientes que ejecutan Windows 7, Windows Server 2008 R2 o Windows Server 2008 deben comprar la Actualización de seguridad extendida para continuar recibiendo actualizaciones de seguridad. Consulte 4522133 para obtener más información.

VULNERABILIDAD CRÍTICA EN ROUTERS CISCO SIN SOPORTE

11/01/2023

MÚLTIPLES VULNERABILIDADES EN LA INTERFAZ DE ADMINISTRACIÓN BASADA EN LA WEB DE LOS ENRUTADORES CISCO SMALL BUSINESS RV016, RV042, RV042G Y RV082

Cisco Small Business RV016, RV042, RV042G, and RV082 Routers Vulnerabilities. (2023, 11 enero). https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5

Cisco ha emitido un aviso de seguridad en donde alerta sobre una vulnerabilidad crítica que afecta a múltiples routers de la compañía que se encuentran al final de su vida útil y de la cual existe una PoC pública, aunque no se conoce por el momento intentos de explotación.

En concreto, esta falla de seguridad registrada como CVE-2023-20025, con un CVSSv3 de 9.0 según fabricante, puede desencadenar en una omisión de autenticación causada por una validación incorrecta de la entrada del usuario dentro de los paquetes HTTP entrantes.

Actores maliciosos no autenticados podrían explotarla remotamente enviando una solicitud HTTP especialmente diseñada a la interfaz de administración de los dispositivos vulnerables. Asimismo, este fallo de seguridad podría encadenarse junto con otra nueva vulnerabilidad, CVE-2023-20026, que posibilitaría la ejecución de código arbitrario. En último lugar, cabe indicar que los dispositivos afectados serían los modelos de router Cisco Small Business RV016, RV042, RV042G y RV082.

Desde Cisco señalan que no publicarán parche, pero como medida paliativa se recomienda deshabilitar la interfaz de administración y bloquear el acceso a los puertos 443 y 60443 para bloquear los intentos de explotación

VULNERABILIDADES CRÍTICAS EN LOS ROUTER NETCOMM Y TP-LINK

15/01/2023

SE HAN DESCUBIERTO UNA SERIE DE VULNERABILIDADES EN LOS ROUTERS NETCOMM Y TP-LINK.

Lakshmanan, R. (2023, 18 enero). Critical Security Vulnerabilities Discovered in Netcomm and TP-Link Routers. The Hacker News. https://thehackernews.com/2023/01/critical-security-vulnerabilities.html

Por un lado, los fallos, identificados como CVE-2022-4873 y CVE-2022-4874, se tratan de un caso de buffer overflow y de omisión de autenticación que permitirían la ejecución remota de código.

El investigador que las descubrió, Brendan Scarvell, ha publicado una PoC para ambas. Los modelos afectados de router serían Netcomm NF20MESH, NF20 y NL1902 que ejecuten versiones de firmware anteriores a R6B035.

Por otro lado, el CERT/CC detalló dos vulnerabilidades que afectan a los router TP-Link WR710N-V1-151022 y Archer-C5-V2-160201, que podrían causar divulgación de información (CVE-2022-4499) y ejecución remota de código (CVE-2022-4498).

NOTICIAS NACIONALES

COMISIÓN DE SEGURIDAD DE LA INFORMACIÓN EN MÉXICO, AÚN SIN LEY DE CIBERSEGURIDAD

20/01/2023

UNA DE LAS GRANDES ASIGNATURAS PENDIENTES DE 2022 FUE LA CREACIÓN DE UNA LEY DE CIBERSEGURIDAD BASADA EN LOS RIESGOS DE CIBERATAQUES REALES Y CADA VEZ MÁS LATENTES EN NUESTRO PAÍS.

Google. (2022, 2 diciembre). Stable Channel Update for Desktop. Chrome Releases. https://chromereleases.googleblog.com/2022/12/stable-channel-update-for-desktop.html

Estamos hablando de la reciente creación de la Comisión Intersecretarial de Tecnologías de la Información y Comunicación, y de la Seguridad de la Información (Comisión ITICSI), que sustituye a la de Desarrollo de Gobierno Electrónico, existente desde 2005, con la diferencia de que a esta nueva se le sumó la tarea primordial de coordinar y conducir acciones para implementar políticas de TI y seguridad de la información de carácter federal.

Hasta este punto podríamos decir que la creación de la Comisión ITICSI es un paso adelante hacia un México Ciberseguro, pero estará en suspenso hasta que haya una Ley de Ciberseguridad que defina las políticas y los lineamientos en materia de Seguridad de la Información para todos los sectores del país, tanto gubernamentales como de iniciativa privada.

sí que, para lograr su misión, se necesitan tres cosas: Una, tener definidas las políticas dentro de la Ley de Ciberseguridad, lo cual está en proceso de delineación, actualmente. Dos, que se amplíe el ámbito de acción de la Comisión hacia Estados y Municipios. Tres, que se promueva, activamente, la integración de los sectores académico, social y privado, más allá de lo establecido en el papel.

Y es que si bien está especificado en el decreto publicado el 10 de enero que podrán invitar a las sesiones de trabajo a representantes de gobiernos estatales y municipales, estos no tendrán voto. Es el mismo caso para los sectores académico, social y privado, que solo tendrán derecho a voz.

VULNERABILIDADES RELEVANTES

TABLA DE VULNERABILIDADES RELEVANTES: ENERO 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-22900	01/31/2023	Improper Neutralization of Special Elements used	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-22900

Descripción: Efence login function has insufficient validation for user input. An unauthenticated remote attacker can exploit this vulnerability to inject arbitrary SQL commands to access, modify or delete database.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-45639	01/23/2023	Improper Neutralization of Special Elements used	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-45639

Descripción: ** DISPUTED ** OS Command injection vulnerability in sleuthkit fls tool 4.11.1 allows attackers to execute arbitrary commands via a crafted value to the m parameter. NOTE: third parties have disputed this because there is no analysis showing that the backtick command executes outside the context of the user account that entered the command line.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-0435	01/22/2023	Excessive Attack Surface	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-0435

Descripción: Excessive Attack Surface in GitHub repository pyload/pyload prior to 0.5.0b3.dev41.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-22884	01/21/2023	Improper Neutralization of Special Elements used	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-22884

Descripción: Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in Apache Software Foundation Apache Airflow, Apache Software Foundation Apache Airflow MySQL Provider.This issue affects Apache Airflow: before 2.5.1; Apache Airflow MySQL Provider: before 4.0.0.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-24028	01/20/2023	Windows Advanced Local Procedure Call (ALPC)	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-24028

Descripción: In MISP 2.4.167, app/Controller/Component/ACLComponent.php has incorrect access control for the decaying import function.

TABLA DE VULNERABILIDADES RELEVANTES: ENERO 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2020-21152	01/20/2023	Improper Neutralization of Special Elements used	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2020-21152

Descripción: SQL Injection vulnerability in inxedu 2.0.6 allows attackers to execute arbitrary commands via the functionIds parameter to /saverolefunction.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-22964	01/20/2023	Improper Authentication	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-22964

Descripción: Zoho ManageEngine ServiceDesk Plus MSP before 10611, and 13x before 13004, is vulnerable to authentication bypass when LDAP authentication is enabled.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-20025	01/19/2023	Improper Neutralization of Special Elements used	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-20025

Descripción: A vulnerability in the web-based management interface of Cisco Small Business RV042 Series Routers could allow an unauthenticated, remote attacker to bypass authentication on the affected device. This vulnerability is due to incorrect user input validation of incoming HTTP packets. An attacker could exploit this vulnerability by sending crafted requests to the web-based management interface. A successful exploit could allow the attacker to gain root privileges on the affected device.

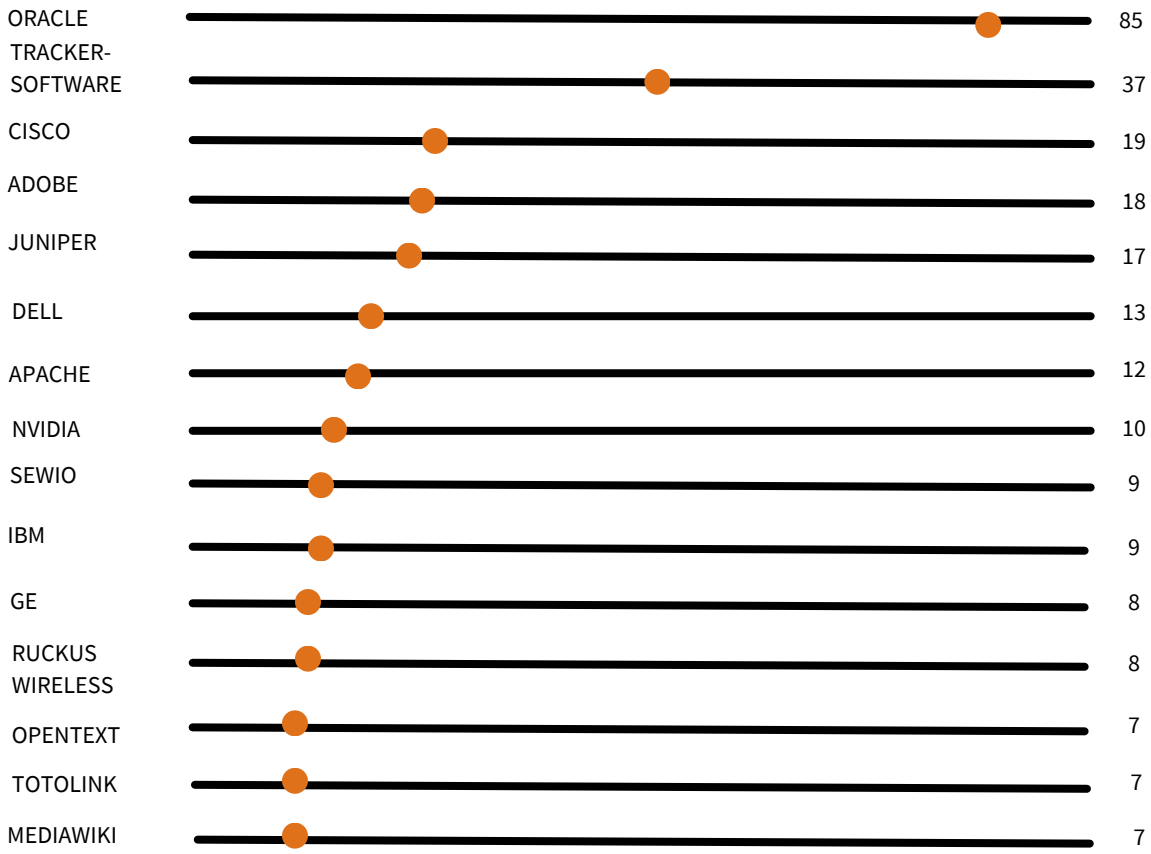
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2014-125083	01/19/2023	Out-of-bounds Write	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2014-125083

Descripción: A vulnerability has been found in Anant Labs google-enterprise-connector-dctm up to 3.2.3 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation of the argument username/domain leads to sql injection. The name of the patch is 6fba04f18ab7764002a1da308e7cd9712b501cb7. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218911.

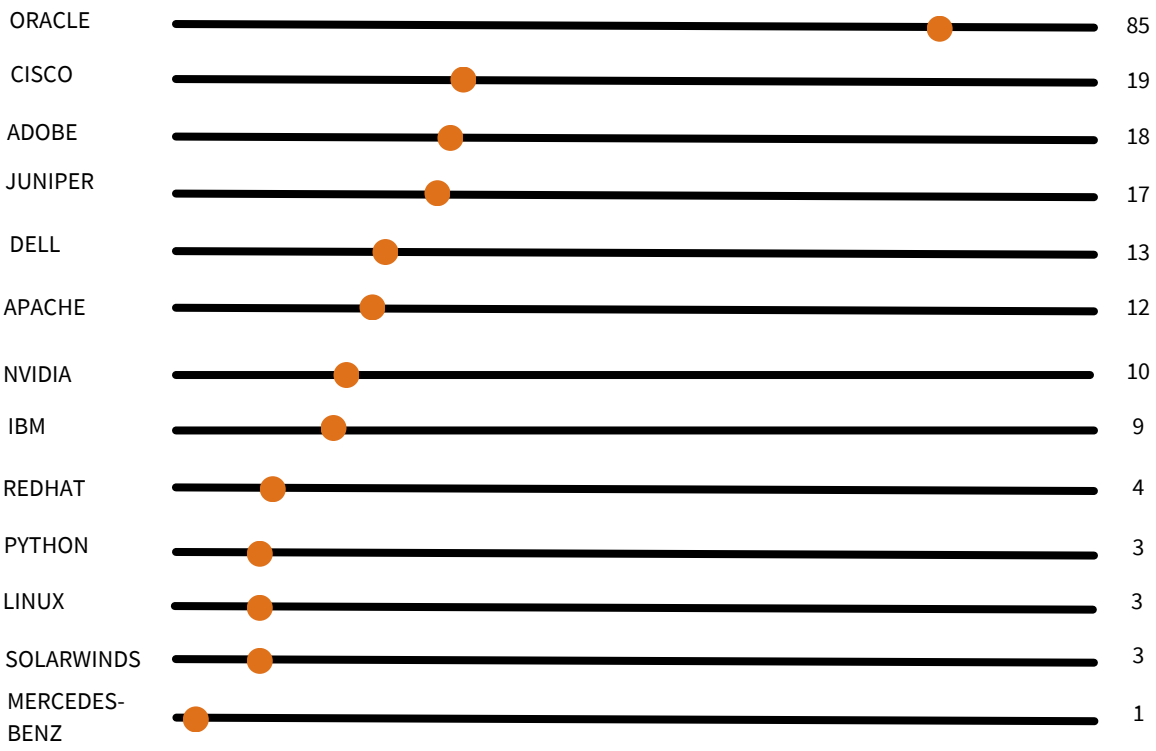
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-34442	01/18/2023	Use of Hard-coded Credentials	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-34442

Descripción: Dell EMC SCG Policy Manager, versions from 5.10 to 5.12, contain(s) a contain a Hard-coded Cryptographic Key vulnerability. An attacker with the knowledge of the hard-coded sensitive information, could potentially exploit this vulnerability to login to the system to gain LDAP user privileges.

FABRICANTES Y SUS VULNERABILIDADES RELEVANTES: ENERO DE 2023



EMPRESAS MULTINACIONALES Y SUS VULNERABILIDADES: ENERO DE 2023



CULTURA DE CIBERSEGURIDAD

¿SABÍAS QUE TU CUENTA DE CORREO TIENE DIRECCIONES ILIMITADAS?

Hay veces que te gustaría saber como es que consiguieron tu correo las campañas de marketing asociadas con spam, en esta nota les muestro una de las formas de poder hacer una regresión y saber cómo es posible esto, es sencillo, solo agregando unos caracteres que pasan o permiten la mayoría de los campos de correo, como lo podrían ser registros a servicios como NETFLIX, NESSUS, etc.

Hay veces que te gustaría saber como es que consiguieron tu correo las campañas de marketing asociadas con spam, en esta nota les muestro una de las formas de poder hacer una regresión y saber cómo es posible esto, es sencillo, solo agregando unos caracteres que pasan o permiten la mayoría de los campos de correo, como lo podrían ser registros a servicios como NETFLIX, NESSUS, etc.

Los ejemplos de combinaciones con el correo son:

ssalgado@gmail.com à ssalgado+lifehacker@gmail.com à ssalgado+gizmodo@gmail.com à ssalgado +facebook@gmail.com à ss.algado @gmail.com à ss.a.lgado@gmail.com à s.s.a.l.g.a.d.o@gmail.com à ssalgado @googlemail.com

Donde el primer correo es el original y los demás son las variantes. La forma en como recibe estas direcciones el servidor de correo es ignorando los signos “+” y “.” añadidos. Enviando a la bandeja del correo sin estos caracteres.

Ahora, en la cabecera del correo, podrás visualizar que correo tomaron para el envío de la información recibida. ¡Espero que esta información te sea de ayuda para poder detectar las campañas de phishing o quien filtra tus datos!

Villamil, C. G. (2016, 28 junio). Truco Gmail: Varias direcciones con la misma cuenta para olvidarse del SPAM. Cinco Días. https://cincodias.elpais.com/cincodias/2016/06/28/lifestyle/1467128625_493652.html

REFERENCIAS

REFERENCIAS

- https://www.synology.com/en-us/security/advisory/Synology_SA_22_26
- https://www.securityjoes.com/post/raspberry-robin-detected-itw-targeting-insurance-financial-institutes-in-europe
- https://www.securityjoes.com/post/raspberry-robin-detected-itw-targeting-insurance-financial-institutes-in-europeNoveno
- https://www.securityjoes.com/post/raspberry-robin-detected-itw-targeting-insurance-financial-institutes-in-europeNoveno
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5
- https://thehackernews.com/2023/01/critical-security-vulnerabilities.html

ZERU

Cybersecurity Services

Security Operation Center - SOC by

ADV

+52 55 6178 9397

contacto@adv-ic.com

Av. Melchor Ocampo 193, Torre Privanza, Piso 11 Oficina 11D
Colonia Veronica Anzures. Delegación Miguel Hidalgo CP 11300