BOLETÍN DE CIBERSEGURIDAD

MAYO 2023

ÍNDICE

NOTICIAS INTERNACIONALES

VULNERABILIDAD CRÍTICA EN LOS FIREWALLS ZYXEL

ZYXEL HA LANZADO PARCHES PARA UNA VULNERABILIDAD DE INYECCIÓN DE COMANDOS DEL SISTEMA OPERATIVO ENCONTRADA POR TRAPA SECURITY E INSTA A LOS USUARIOS A INSTALARLOS PARA UNA PROTECCIÓN ÓPTIMA.

Zyxel security advisory for OS command injection vulnerability of firewalls | Zyxel Networks. (s. f.). https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-remote-command-injection-vulnerability-of-firewalls

¿Qué son las vulnerabilidades?

El manejo inadecuado de mensajes de error en algunas versiones de firewall podría permitir que un atacante no autenticado ejecute algunos comandos del sistema operativo de forma remota mediante el envío de paquetes manipulados a un dispositivo afectado.

¿Qué versiones son vulnerables y qué debe hacer?

Después de una investigación exhaustiva, identificamos los productos vulnerables que se encuentran dentro de su período de soporte de vulnerabilidad y lanzamos parches para abordar la vulnerabilidad, como se muestra en la tabla a continuación

VULNERABILIDAD DE EJECUCIÓN DE COMANDOS REMOTOS DE ADAPTADORES TELEFÓNICOS DE 2 PUERTOS CISCO SPA112

UNA VULNERABILIDAD EN LA INTERFAZ DE ADMINISTRACIÓN BASADA EN WEB DE LOS ADAPTADORES DE TELÉFONO DE 2 PUERTOS CISCO SPA112 PODRÍA PERMITIR QUE UN ATACANTE REMOTO NO AUTENTICADO EJECUTE CÓDIGO ARBITRARIO EN UN DISPOSITIVO AFECTADO.

Cisco SPA112 2-Port Phone Adapters Remote Command Execution Vulnerability. (2023, 3 mayo). https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-unauth-upgrade-UqhyTWW

Esta vulnerabilidad se debe a la falta de un proceso de autenticación dentro de la función de actualización del firmware . Un atacante podría aprovechar esta vulnerabilidad actualizando un dispositivo afectado a una versión modificada del firmware. Una explotación exitosa podría permitir que el atacante ejecute código arbitrario en el dispositivo afectado con todos los privilegios .

VULNERABILIDADES EN PLATAFORMAS CLOUD

EL EQUIPO DE INVESTIGADORES DE OTORIO DESCUBRIÓ 11 VULNERABILIDADES QUE AFECTAN A DIFERENTES PROVEEDORES DE PLATAFORMAS DE ADMINISTRACIÓN DE CLOUD.

Vulnerabilities Jeopardize Users of Major Industrial Cellular Routers Cloud Management Platforms. (s. f.). https://www.otorio.com/news-events/news/vulnerabilities-jeopardize-users-of-major-industrial-cellular-routers-cloud-management-platforms/

En concreto, se tratan de Sierra Wireless, Teltonika Networks e InHand Networks las compañías afectadas.

En relación con los fallos de seguridad los que afectan a Teltonika Networks son CVE-2023-32346, CVE-2023-32347, CVE-2023-32348, CVE-2023-2586, CVE-2023-2587 y CVE-2023-2588 identificados en el sistema de administración remota (RMS), su explotación podría exponer información confidencial y permitir la ejecución remota de código (RCE).

En relación con las vulnerabilidades en InHand Networks, CVE-2023-22600, CVE-2023-22598, CVE-2023-22599, CVE-2023-22597 y CVE-2023-2261 podrían ser aprovechadas por actores maliciosos para realizar RCE.

En último lugar, los fallos identificados en Sierra Wireless, CVE-2023-31279 y CVE-2023-31280, podrían permitir a un atacante buscar dispositivos no registrados que estén conectados a la nube, obtener sus números de serie y registrarlos en una cuenta bajo su control con el objetivo de ejecutar comandos.

GITLAB PARCHEA UNA VULNERABILIDAD CRÍTICA

GITLAB HA ABORDADO UNA VULNERABILIDAD CRÍTICA QUE AFECTA A GITLAB COMMUNITY EDITION (CE) Y ENTERPRISE EDITION (EE) EN LA VERSIÓN 16.0.0.

GitLab Critical Security Release: 16.0.1. (2023, 23 mayo). GitLab. https://about.gitlab.com/releases/2023/05/23/critical-security-release-gitlab-16-0-1-released/

En concreto, dicho fallo de seguridad ha sido registrado como CVE-2023-2825, CVSSv3 de 10, y fue descubierto por un investigador de seguridad llamado pwnie. En cuanto a la causa del fallo este surge de un problema de cruce de rutas que podrían permitir a un atacante no autenticado leer archivos arbitrarios en el servidor cuando existe un archivo adjunto en un proyecto público anidado dentro de al menos cinco grupos.

Por tanto, la explotación de esta vulnerabilidad podría desencadenar en la exposición de datos confidenciales como códigos de software patentados, credenciales de usuario, tokens, archivos y otra información privada. Desde GitLab recomiendan a sus usuarios actualizar a la última versión, 16.0.1, para solucionar este problema de seguridad.

ZYXEL CORRIGE DOS VULNERABILIDADES CRÍTICAS QUE AFECTAN A SUS FIREWALLS13

ZYXEL HA LANZADO PARCHES PARA FIREWALLS AFECTADOS POR MÚLTIPLES VULNERABILIDADES DE DESBORDAMIENTO DE BÚFER. SE RECOMIENDA A LOS USUARIOS QUE LOS INSTALEN PARA UNA PROTECCIÓN ÓPTIMA.

Zyxel security advisory for multiple buffer overflow vulnerabilities of firewalls | Zyxel Networks. (s. f.). https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-buffer-overflow-vulnerabilities-of-firewalls

CVE-2023-33009
Una vulnerabilidad de desbordamiento de búfer en la función de notificación en algunas versiones de firewall podría permitir que un atacante no autenticado provoque condiciones de denegación de servicio (DoS) e incluso una ejecución remota de código en un dispositivo afectado.

CVE-2023-33010
Una vulnerabilidad de desbordamiento de búfer en la función de procesamiento de ID en algunas versiones de firewall podría permitir que un atacante no autenticado provoque condiciones DoS e incluso una ejecución remota de código en un dispositivo afectado.

¿Qué versiones son vulnerables y qué debe hacer?

Después de una investigación exhaustiva, identificamos las series de firewall vulnerables que se encuentran dentro de su período de soporte de vulnerabilidad y lanzamos parches para abordar la vulnerabilidad, como se muestra en la tabla a continuación.

VULNERABILIDAD EN KEEPASS PERMITE RECUPERAR CONTRASEÑAS MAESTRAS

INVESTIGADORES DE SEGURIDAD HAN PUBLICADO UN ARTÍCULO SOBRE UNA NUEVA VULNERABILIDAD QUE PERMITE RECUPERAR LAS CONTRASEÑAS MAESTRAS EN EL GESTOR DE CONTRASEÑAS KEEPASS.

KeePass. (s. f.). https://sourceforge.net/p/keepass/discussion/329220/thread/a146e5cf6b/

La vulnerabilidad ha sido clasificada como CVE-2023-32784 y afecta a las versiones 2.x de KeePass para Windows, Linux y macOS. Se espera que sea parcheada en la versión 2.54, asimismo, cabe indicar que dicho fallo de seguridad cuenta con una PoC disponible. Para su explotación, no importa de dónde provenga la memoria, y si el espacio de trabajo está bloqueado o no. Además, también es posible volcar la contraseña desde la RAM cuando KeePass ya no se esté ejecutando.

Cabe destacar que la explotación exitosa del fallo se basa en la condición de que un atacante ya haya vulnerado el equipo de un objetivo potencial y que se requiere que la contraseña se escriba en un teclado y no se copie desde el portapapeles del dispositivo.

NOTICIAS NACIONALES

MÉXICO OCUPA CUARTO LUGAR EN PAÍSES QUE MÁS PAGAN POR ATAQUES DE 'RANSOMWARE'

MÉXICO ES EL CUARTO PAÍS DE LATINOAMÉRICA QUE MÁS CIBERATAQUES POR RANSOMWARE PAGA, SITUACIÓN QUE PREOCUPA A LA EMPRESA DE CIBERSEGURIDAD TREN MICRO, YA QUE POR CADA VÍCTIMA LOS CIBERCRIMINALES PUEDEN FINANCIAR ENTRE SEIS Y DIEZ ATAQUES SIN NECESIDAD DE COBRAR A OTRA.

Rodríguez, S. (2023, 31 mayo). México ocupa cuarto lugar en países que más pagan por ataques de «ransomware». Grupo Milenio. https://www.milenio.com/negocios/mexico-ocupa-cuarto-paises-pagan-ciberataques

Explicó que es lo mismo que pasa con los secuestros de personas, en cuanto más se paga, los secuestradores siguen financiando y funcionando, por lo que cada vez que se paga un rescate, no es recuperar los datos, sino que con ello se permite que la prese opere y después hay extorsiones sobre el hacer pública información que puede ser muy crítica para que el negocio siga funcionando.

Agregó que los grupos de atacantes normalmente ven cuánto es la facturación de la empresa y al ver cuánto ganan, por ejemplo, cobran 5 por ciento del total, cuyo porcentaje puede ser de millones de dólares, “ellos calculan, es toda una industria, y tienen elementos que se dedican a la negociación”, dijo.

Juan Pablo Castro añadió que algo muy importante es que el secuestro de información es un negocio que se basa en la reputación y si tal información se publica nadie más va a pagar por ello y el daño es sólo para el agente atacado, “esto es de códigos entre criminales”.

Aclaró que es difícil saber cuál es la cantidad que se paga por ataques de ransomware y, además, no todas las empresas dicen que pagaron un ataque, pero se sabe que hubo tal pago porque los atacantes dejan de publicar los datos que tenían. Otra forma de saber que hubo un pago es porque las empresas operan en distintos países y las legislaciones en algunos de ellos los obligan a decir que fueron víctimas de ataques o porque son empresas públicas y deben de informarlo.

VULNERABILIDADES RELEVANTES

TABLA DE VULNERABILIDADES RELEVANTES: MAYO 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-2951	05/28/2023	Improper Neutralization of Special Elements	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-2951

Descripción: A vulnerability classified as critical has been found in code-projects Bus Dispatch and Information System 1.0. Affected is an unknown function of the file delete_bus.php. The manipulation of the argument busid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-230112.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2022-48479	05/26/2023	Out-of-bounds Read	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-48479

Descripción: The facial recognition TA of some products has the out-of-bounds memory read vulnerability. Successful exploitation of this vulnerability may cause exceptions of the facial recognition service.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2021-46887	05/26/2023	Other	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2021-46887

Descripción: Lack of length check vulnerability in the HW_KEYMASTER module. Successful exploitation of this vulnerability may cause out-of-bounds read.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-30145	05/26/2023	Improper Control of Generation of Code ('Code Injection')	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2022-20532

Descripción: Camaleon CMS v2.7.0 was discovered to contain a Server-Side Template Injection (SSTI) vulnerability via the formats parameter.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-33280	05/26/2023	Improper Neutralization of Special Elements	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-33280

Descripción: In the Store Commander scquickaccounting module for PrestaShop through 3.7.3, multiple sensitive SQL calls can be executed with a trivial HTTP request and exploited to forge a blind SQL injection.

TABLA DE VULNERABILIDADES RELEVANTES: MAYO 2023

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-33278	05/24/2023	Improper Neutralization of Special Elements	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-33278

Descripción: In the Store Commander scexportcustomers module for PrestaShop through 3.6.1, sensitive SQL calls can be executed with a trivial HTTP request and exploited to forge a blind SQL injection.

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-2851	05/25/2023	Improper Neutralization of Special Elements	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-2851

Descripción: ** UNSUPPPORTED WHEN ASSIGNED ** Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in AGT Tech Ceppatron allows Command Line Execution through SQL Injection, SQL Injection.This issue affects all versions of the sofware also EOS when CVE-ID assigned

Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-2887	05/25/2023	Authentication Bypass by Spoofing	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-2887

Descripción: Authentication Bypass by Spoofing vulnerability in CBOT Chatbot allows Authentication Bypass.This issue affects Chatbot: before Core: v4.0.3.4 Panel: v4.0.3.7.

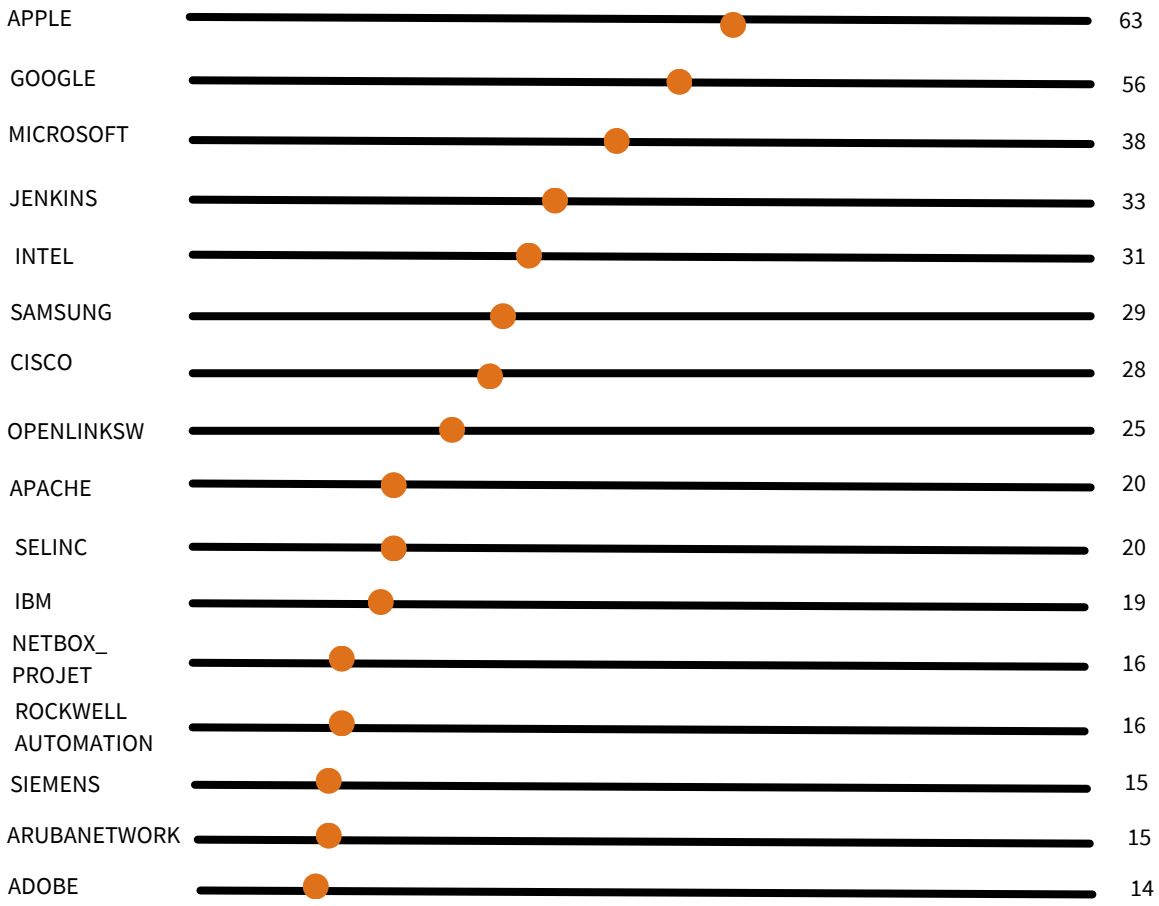
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-2884	05/25/2023	Use of Insufficiently Random Values	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-2884

Descripción: Rengine v1.0.2 was discovered to contain a remote code execution (RCE) vulnerability via the yaml configuration function.

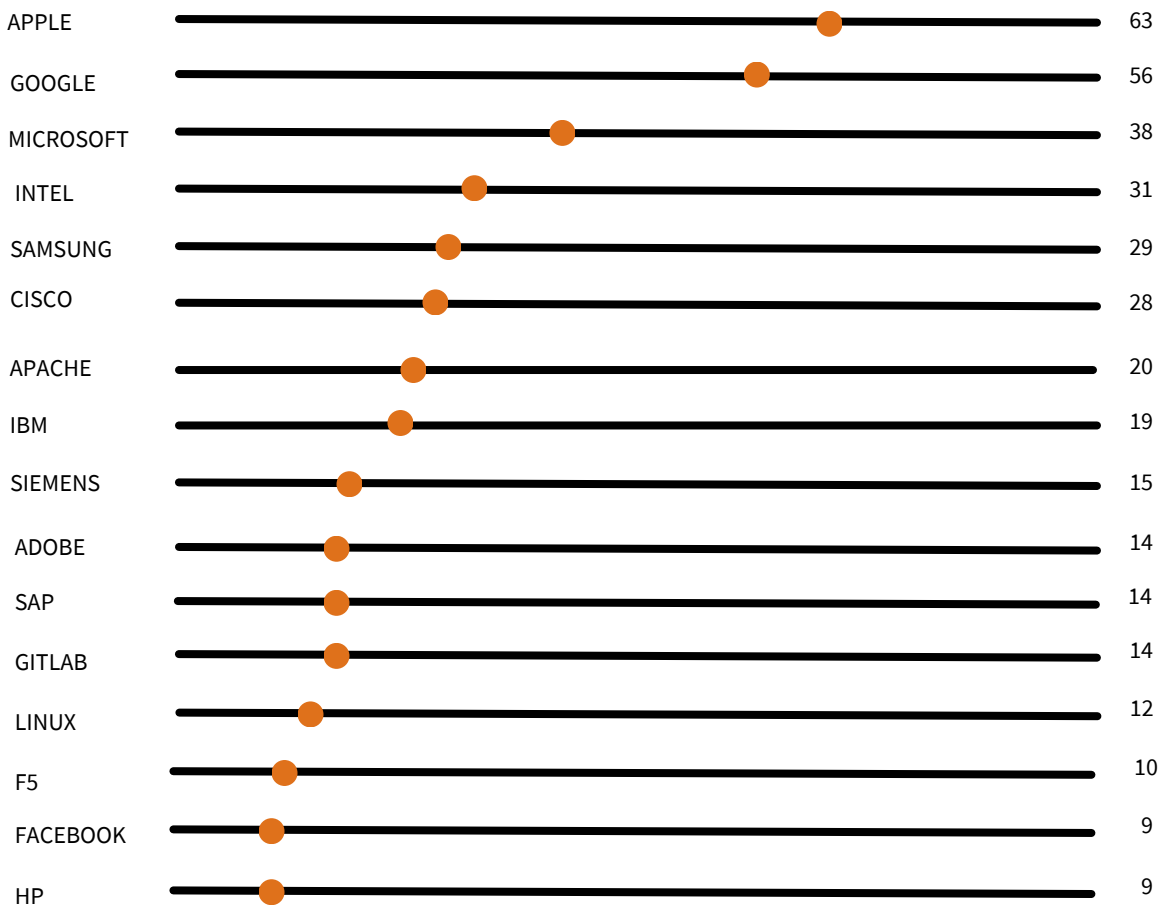
Identificador	Fecha de publicación	Título	CVSS v3.x	Referencias
CVE-2023-2734	05/20/2023	Authentication Bypass Using an Alternate Path or Channel	CVSS v3.1:9.8 [critical]	https://nvd.nist.gov/vuln/detail/CVE-2023-2734

Descripción: The MStore API plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 3.9.1. This is due to insufficient verification on the user being supplied during the cart sync from mobile REST API request through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the user id.

FABRICANTES Y SUS VULNERABILIDADES RELEVANTES: MAYO DE 2023



EMPRESAS MULTINACIONALES Y SUS VULNERABILIDADES: MAYO DE 2023



CULTURA DE CIBERSEGURIDAD

USO DE CORREO CORPORATIVO PARA USO PERSONAL.

El uso del correo electrónico, así como cualquier red social, debe hacerse con mucho cuidado.

El correo es una forma de identificarnos en línea, pero cuando se trata de un correo corporativo podemos dar demasiada información a personajes maliciosos que buscan poder accesar a la red de una compañía, corporación o empresa.

Como bien se sabe, cuando un nuevo empleado ingresa a una compañía, corporación o empresa, generalmente se le asigna un correo corporativo. Este correo contiene el dominio de la compañía (la parte que viene después del "@". Por ejemplo: pedro.perez@seguroselcaballo.com)
Con este correo se tendrá comunicación tanto interna (compañeros dentro de la misma compañía con el mismo dominio) así como comunicación externa (clientes, proveedores, etc, con dominios que no pertenecen a la compañía. Por ejemplo: juan.juarez@llanteramiami.com).

Teniendo en mente esto, podemos tener la idea de que en esta comunicación mencionada tanto interna como externa se puede manejar información clasificada, sensible y muy importante.
Enlistaremos algunas situaciones de riesgo que se podrían suscitar con el incorrecto uso de los correos corporativos:

- Filtración de información por envío de correos a dominios externos no relacionados a la compañía: Como se comentó, dentro de las empresas se maneja información sensible, importante y muchas veces confidencial. El usuario debe ser consciente que el mal manejo de dicha información puede ser un delito. Si no es necesario, evitar enviar o reenviar correos a dominios externos tales como @outlook.com, @gmail.com, @hotmail.com, ya que cualquier persona tiene acceso para crear cuentas en estos dominios y sería fácil realizar una suplantación. Cerciorarse que, en caso de enviar correos a dominios externos tengan relación con su compañía y sean autorizados (para ello puede acudir al área correspondiente de su lugar de trabajo).

- Registrar el correo corporativo en sitios web sin relación con la compañía: Uno de los errores que los empleados de una compañía pueden realizar es registrar su correo corporativo en un sitio web que no tenga relación laborar con la compañía. Por ejemplo, registrar su correo en sitios de tiendas online le generará correos "spam" sobre ofertas y promociones. Esto puede provocar que el espacio de almacenamiento sea ocupado por completo en poco tiempo y esto será un problema. Este ejemplo puede también verse con sitios bancarios, sitios de stream, entre otros.

- Registrar el correo corporativo en sitios web infectados con malware: En el peor de los casos, el correo electrónico corporativo puede llegar a ser registrado en un sitio web infectado de malware. En estos casos el correo se puede llegar a ver comprometido de una manera demasiado peligrosa. Pueden obtener la información de su dominio y suplantar usuarios dentro de la empresa, mandando correos que parecen "legítimos" pero que sólo buscan engañar y obtener información "secreta" que pueden utilizar para obtener ingresos monetarios, ya sea como estafa, chantaje, secuestro de información o hacerla pública. De igual forma se puede convertir en un blanco de ataques directos a su cuenta de correo (intentos de inicio de sesión por fuerza bruta/ataque de diccionario, phishing, entre otros).

USO DE CORREO CORPORATIVO PARA USO PERSONAL.

- Caer en phishing: En algunas ocasiones, se pueden llegar a recibir correos de lo que aparentan ser sitios “reales”, “oficiales” o “verídicos” (suplantando a Microsoft / Office365). En estos correos se les solicita iniciar sesión con sus credenciales, lo cual es para realmente obtenerlas, entrar a sus cuentas y realizar lo que les plazca a los actores maliciosos. Para ello es importante siempre acudir al área correspondiente en su lugar de trabajo para notificar este tipo de correos antes de realizar cualquier otra opción.

Algunas recomendaciones a las empresas para reducir el riesgo de los puntos anteriores es crear, fomentar y difundir las campañas de aprendizaje sobre phishing y el correcto uso de cuentas corporativas. Hacer ver a los trabajadores los riesgos que existen y también sus consecuencias.

Otra forma de proteger su cuenta corporativa es usas el Doble factor de autenticación (o MFA).
Por último, es importante recordar que, ante cualquier correo sospechoso recibido, lo primero que debe hacerse es acudir al área correspondiente de su lugar de trabajo y reportarlo.

REFERENCIAS

REFERENCIAS

- https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-remote-command-injection-vulnerability-of-firewalls
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-unauth-upgrade-UqhyTWW
- https://www.otorio.com/news-events/news/vulnerabilities-jeopardize-users-of-major-industrial-cellular-routers-cloud-management-platforms/
- https://about.gitlab.com/releases/2023/05/23/critical-security-release-gitlab-16-0-1-released/
- https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-buffer-overflow-vulnerabilities-of-firewalls
- https://sourceforge.net/p/keepass/discussion/329220/thread/a146e5cf6b/
- https://www.milenio.com/negocios/mexico-ocupa-cuarto-paises-pagan-ciberataques

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