BOLETÍN INFORMATIVO 14-21SEP2023

CONCIBER

Comité Nacional de Seguridad Cibernética

Boletín de Ciberseguridad

ESET	Amenazas cibernéticas en Guatemala	IMPORTANTE

Según plataforma VIRUS RADAR de ESET la amenaza cibernética que prevaleció en Guatemala durante la semana 14-21SEP2023 fue el protocolo SMB (7.58 %) seguido del vector HTML/Scrinject (5.76 %).

Principales amenazas cibernéticas en Guatemala
14-21SEP2023

	Threat Name	Change	Prevalence Level
1	SMB.Attack.Bruteforce	▼	7.58 %
2	HTML/ScrInject	▲	5.76 %
3	JS/Adware.Adport	▼	5.21 %
4	JS/Packed.Agent.L	▼	4.1 %
5	JS/Packed.Agent.K	▼	4.04 %
6	RDP.Attack.Bruteforce	▼	3.22 %
7	Win32/Phorpiex	▼	2.92 %
8	Android/Packed.TencentProtect.D	▼	2.43 %
9	JS/Adware.TerraClicks	▼	2.39 %
10	JS/Adware.Popcash	▼	2.08 %

Fuente: Virus Radar

https://virusradar.com/en/statistics/10

CISCO	**Cisco VPN Routers presentó fallas de consideración**	**CRÍTICO (Puntuación CVSS de 8,9)**

14SEP2023 35 fallas arbitrarias de escritura de archivos y ataques de ejecución remota de código (RCE) provocaron denegación de servicios (DDoS). Los routers afectados son vulnerables a los ataques si se ejecuta una versión de firmware anterior a la versión 1.0.01.02. Las fallas en la interfaz de administración del router, podrían propiciar que un atacante remoto autenticado ejecute un código arbitrario, provocando una denegación de servicio. Los recursos que se ven afectados se encuentran los modelos RV110W, RV130W, RV215W, VPN RV160, RV260, RV260P y RV260W.

https://sec.cloudapps.cisco.com/security/center/publicationListing.x?product=Cisco&impac=critical&sort=-day_sir#~Vulnerabilities

FORTINET	**Fortinet parchó vulnerabilidades en productos FortiOS, FortiProxy y FortiWeb**	**CRÍTICO (Puntuación CVSS de 7,1)**

14SEP2023 Vulnerabilidad de fallo de seguridad CVE-2023-29183 provocó la neutralización inadecuada de la entrada durante la generación de la página web del administrador. La falla afectó las versiones 7.0.x y 7.2.x de FortiProxy, y 6.2.x, 6.4.x, 7.0.x y 7.2.x de FortiOS. Fortinet lanzó las versiones 7.0.11 y 7.2.5 de FortiProxy, y 6.2.15, 6.4.13, 7.0.12, 7.2.5 y 7.4.0 de FortiOS para solucionar el problema.

Fortinet lanzó parches para el problema de alta gravedad CVE-2023-34984 en su firewall de aplicaciones web y solución de protección API FortiWeb, el fallo podría permitir a un atacante eludir las protecciones XSS y falsificación de solicitudes entre sitios (CSRF) existentes. El error afectó a las versiones 6.3, 6.4, 7.0.x y 7.2.x de FortiWeb y se solucionó con el lanzamiento de las versiones 7.0.7 y 7.2.2 de FortiWeb.

https://www.securityweek.com/fortinet-patches-high-severity-vulnerabilities-in-fortios-fortiproxy-fortiweb-products/?web_view=true

	Alerta por Seguridad de módulos en Wordpress	**CRÍTICO (Puntuación CVSS de 7,8)**

15SEP2023 Sitios web desarrollados con el administrador de contenidos CMS WordPress fueron contaminados por malware que afectó diversos temas (templates) y plugins. Estas funciones son programadas por terceros y agregadas al CMS de acuerdo a la información proporcionada por Wordfence. Esta versión del malware WP-VCD es una cepa de infecciones dirigidas a WordPress conocidas por su uso de temas pirateados para su distribución.

Wordfence ha detectado alrededor de 20 millones de archivos maliciosos en más de 1.2 millones de sitios de WordPress durante 2023.

https://ithemes.com/blog/wordpress-vulnerabilities-explained/

	Google parchó vulnerabilidad crítica de Chrome «Actualizar ahora»	**CRÍTICO (Puntuación CVSS de 8,8)**

15SEP2023 Google lanzó parches de seguridad para corregir una falla de seguridad crítica en su navegador web Chrome que ha sido explotada y aprovechada por actores de amenazas. La vulnerabilidad CVE-2023-4863, se ha descrito como un caso de desbordamiento del búfer que reside en el formato de imagen WebP y que podría provocar la ejecución de código arbitrario o un bloqueo. La explotación exitosa de esta falla permitiría a un atacante remoto realizar una escritura en memoria fuera de los límites a través de una página HTML diseñada.

Google señaló que existe un exploit para esta vulnerabilidad y recomendó a los usuarios actualizar a la versión 116.0.5845.187/.188 de Chrome para Windows y 116.0.5845.187 para macOS y Linux para mitigar posibles amenazas.

https://nvd.nist.gov/vuln/detail/CVE-2023-4863|
https://developers.google.com/speed/webp?hl=es-419
https://thehackernews.com/2023/09/google-rushes-to-patch-critical-chrome.html

SAP Business One	Vulnerabilidad en Interfaz html de SAP Business Objects Business Intelligence Platform 420 Web Intelligence	**CRÍTICO (Puntuación CVSS de 7,3)**

16SEP2023 Vulnerabilidad CVE-2023-42472 identificada por SAP Business ONE fue categorizada como crítica. La falla afecta en el procesamiento desconocido del componente *Interfaz HTML de Web Intelligence*.

La explotación exitosa de la falla permite al actor de amenazas cargar o transferir archivos maliciosos que pueden procesarse automáticamente dentro del entorno del producto vulnerando la confidencialidad, integridad y disponibilidad del servicio. Se desconoce si existe un exploit dirigido a explotar esta vulnerabilidad.

https://vuldb.com/es/?id.239525

	Posibles fraudes por mensajería de WhatsApp	**IMPORTANTE**

16SEP23 Casos de intrusión a WhatsApp a través del envío de un mensaje de texto con el código 991-210 y link https://v.whatsapp[.]com/991210?s=1. Las victimas reciben un mensaje solicitando el reenvío del código tras lo que pierden el control de su cuenta, produciéndose un «secuestro virtual».

Microsoft	Microsoft lanzó parches para 59 vulnerabilidades	**IMPORTANTE**

21SEP2023 Microsoft emitió 59 parches de actualización para corregir vulnerabilidades en distintos servicios que permiten a un atacante ejecutar remotamente código malicioso. La explotación exitosa de los fallos, podría conducir a un actor de amenazas a ejecutar códigos arbitrarios y a una pérdida total de la integridad de los sistemas y servicios.

https://msrc.microsoft.com/update-guide/releaseNote/2023-Sep