Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

TETÃ REKUÁI GOBIERNO NACIONAL

BOLETÍN DE ALERTA

Boletín Nro.: 2020-31

Fecha de publicación: 16/10/2020

Tema: Actualizaciones de seguridad en SonicWall VPN abordan una vulnerabilidad crítica.

Sistemas Afectados:

- SonicOS en versiones 6.5.4.7-79n y anteriores;
- SonicOS en versiones 6.5.1.11 y anteriores;
- SonicOS en versiones 6.0.5.3-93o y anteriores;
- SonicOSv en versiones 6.5.4.4-44v-21-794 y anteriores;
- SonicOS versión 7.0.0.0-1

Descripción:

Investigadores de seguridad han descubierto recientemente una vulnerabilidad de **riesgo crítico** que afecta a diversas versiones de **SonicOS** ejecutadas en miles de **VPNs (Virtual Private Networks) activas**.

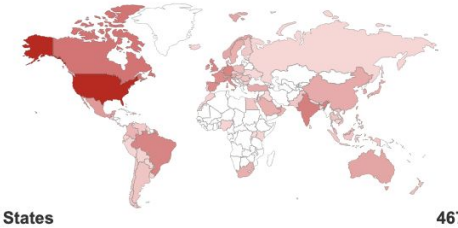
El fallo ha sido identificado con el CVE-2020-5135 y trata de una vulnerabilidad de tipo Stack-based Buffer Overflow en el **portal VPN** del dispositivo de seguridad de red **SonicWall**. Un atacante remoto no autenticado podría explotar exitosamente este fallo enviando **solicitudes HTTP especialmente diseñadas** con un controlador de protocolo personalizado, a un dispositivo vulnerable.

Los **detalles técnicos** de esta vulnerabilidad aún no han sido revelados. Sin embargo, los investigadores de seguridad resaltan la importancia de aplicar los **parches de seguridad** lanzados por **SonicWall**, lo antes posible. Esto debido a que, mediante una búsqueda en **Shodan** se pudo observar que casi **800 mil hosts** podrían estar afectados y ser vulnerables a este fallo, a continuación se visualiza una imagen con los resultados de la búsqueda y los principales paises afectados:

TOTAL RESULTS

771,348

TOP COUNTRIES

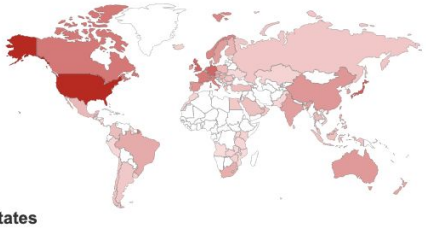


United States	467,592
Canada	40,178
India	25,392
United Kingdom	23,153
Germany	21,867

TOTAL RESULTS

24,326

TOP COUNTRIES



United States	11,811
Japan	2,090
United Kingdom	1,688
Germany	1,613
Canada	806

Específicamente en **Paraguay**, se pudieron visualizar un total de **147 hosts potencialmente vulnerables** a este fallo con la consulta de búsqueda **product:"SonicWALL firewall http config" country:PY** en Shodan. Sin embargo, cabe recalcar que dichas búsquedas representan a **servidores SonicWall conectados a internet** y como sus respectivas versiones no han podido ser determinadas, no está claro si los mismos son vulnerables.

TOTAL RESULTS

147

TOP COUNTRIES

Paraguay	147

TOP CITIES

Asunción	81
San Lorenzo	13
Alto Vera	6
Lambaré	5
San Antonio	4

Por otro lado, **SonicWall** ha abordado también otras **10 vulnerabilidades**, de las cuales 7 han sido catalogadas con **riesgo alto** y 3 con **medio**, de las cuales podemos destacar múltiples vulnerabilidades que podrían permitir a un atacante **remoto no autenticado** realizar ataques de **denegación de servicios (DoS)** en **SonicOS** (CVE-2020-5133) y en el **servicio Firewall SSLVPN** de **SonicOS** (CVE-2020-5137,CVE-2020-5138).

Impacto:

La explotación exitosa podría permitir podría permitir a un atacante **remoto no autenticado** para realizar ataques de **denegación de servicios (DoS)** y potencialmente ejecutar código arbitrario.

Solución y prevención:

- Actualizar los **productos afectados** desde la página oficial de SonicWall, a las siguientes versiones:
    - SonicOS 6.5.4.7-83n;
    - SonicOS 6.5.1.12-1n;
    - SonicOS 6.0.5.3-94o;
    - SonicOS 6.5.4.v-21s-987;
    - Gen 7 7.0.0.0-2 y posteriores.

Información adicional:

- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2020-0010
- https://es-la.tenable.com/blog/cve-2020-5135-critical-sonicwall-vpn-portal-stack-based-buffer-overflow-vulnerability
- https://www.bleepingcomputer.com/news/security/critical-sonicwall-vulnerability-affects-800k-firewalls-patch-now/