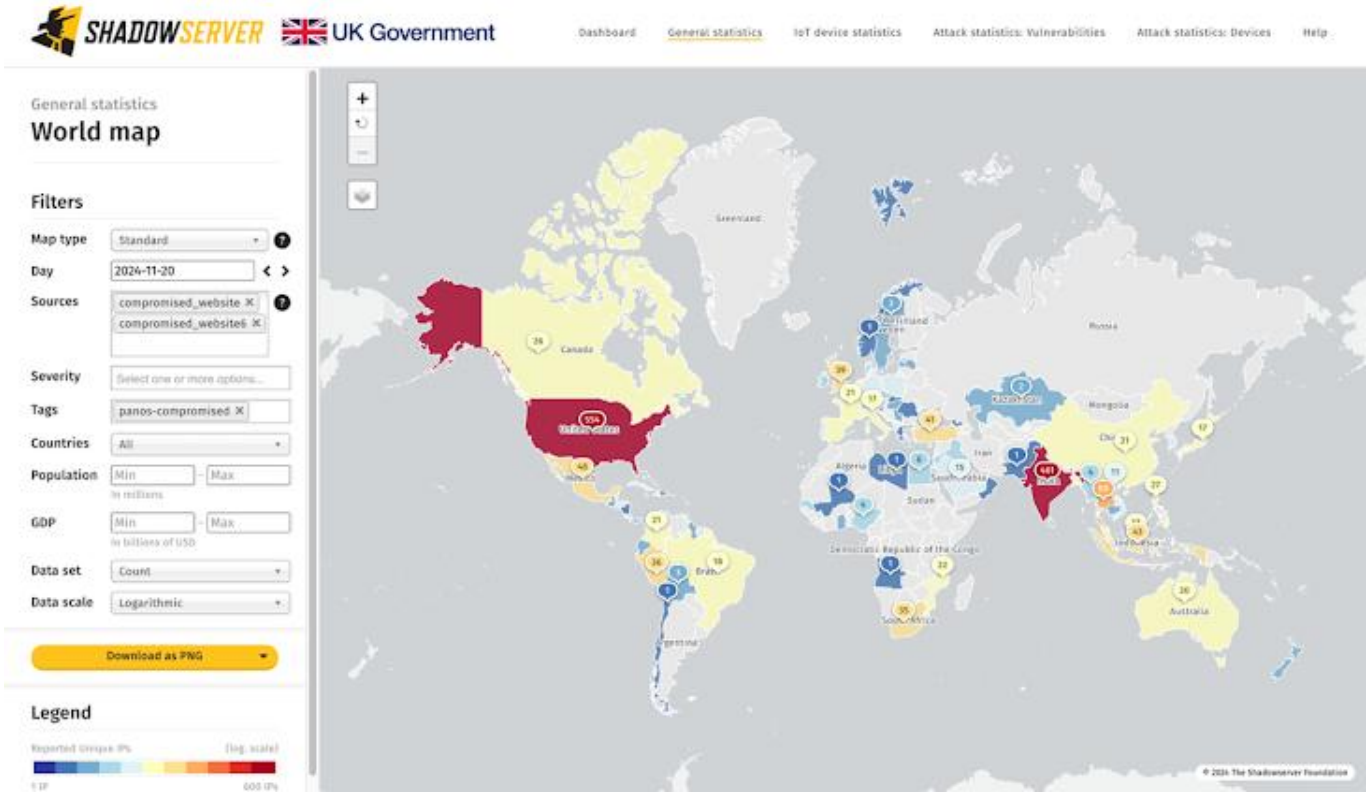
Se calcula que alrededor de 2,000 dispositivos de Palo Alto Networks han sido afectados en una campaña que explota activamente vulnerabilidades de seguridad recientemente identificadas.

Según datos de la Fundación Shadowserver, la mayor parte de las infecciones se han registrado en los Estados Unidos (554) e India (461), seguidos por Tailandia (80), México (48), Indonesia (43), Turquía (41), el Reino Unido (39), Perú (36) y Sudáfrica (35).

A principios de esta semana, Censys informó haber detectado 13,324 interfaces de gestión de cortafuegos de nueva generación (NGFW) expuestas públicamente, con un 34% de estas localizadas en los Estados Unidos. Sin embargo, no todos los sistemas expuestos presentan vulnerabilidades.

Las fallas de seguridad, identificadas como CVE-2024-0012 (puntuación CVSS: 9.3) y CVE-2024-9474 (puntuación CVSS: 6.9), combinan una omisión de autenticación y una escalada de privilegios. Esto permite a los atacantes realizar acciones maliciosas, como alterar configuraciones o ejecutar código arbitrario.




Palo Alto Networks, que ha denominado a esta explotación inicial *«Operación Lunar Peek,»* señaló que las vulnerabilidades están siendo utilizadas para ejecutar comandos y desplegar malware, como shells web basados en PHP, en dispositivos comprometidos.

La compañía advirtió que los ciberataques dirigidos a estas fallas probablemente aumentarán con la disponibilidad de un exploit que combina ambas vulnerabilidades.

De hecho, la empresa afirmó con un nivel de confianza moderado a alto que existe un exploit funcional que vincula las vulnerabilidades CVE-2024-0012 y CVE-2024-9474, lo que podría ampliar la actividad maliciosa.

Asimismo, observó actividad de escaneo tanto manual como automatizado, enfatizando la importancia de que los usuarios instalen las actualizaciones de seguridad más recientes de inmediato y protejan el acceso a la interfaz de administración siguiendo las mejores prácticas

recomendadas.

Esto incluye, en particular, limitar el acceso exclusivamente a direcciones IP internas de confianza para evitar accesos no autorizados desde internet.