Cisco ha emitido una advertencia sobre un aumento significativo a nivel mundial en los ataques de fuerza bruta dirigidos a una variedad de dispositivos, incluidos los servicios de Red Privada Virtual (VPN), las interfaces de autenticación de aplicaciones web y los servicios SSH, desde al menos el 18 de marzo de 2024.

Según Cisco Talos, estos ataques parecen estar originándose desde nodos de salida de TOR y diversos túneles y proxies de anonimización.

La compañía de ciberseguridad ha destacado que los ataques exitosos podrían resultar en accesos no autorizados a la red, bloqueos de cuentas o condiciones de denegación de servicio.

Los objetivos de los ataques, descritos como amplios y oportunísticos, incluyen dispositivos como:

- Cisco Secure Firewall VPN
- Checkpoint VPN
- Fortinet VPN
- SonicWall VPN
- Servicios de RD Web
- Mikrotik
- Draytek
- Ubiquiti

Según los informes de Cisco Talos, los intentos de fuerza bruta están utilizando tanto nombres de usuario genéricos como válidos para organizaciones específicas. Estos ataques están dirigidos indiscriminadamente a una amplia variedad de sectores en distintas regiones geográficas.

Las direcciones IP de origen de este tráfico suelen estar asociadas con servicios de proxy como TOR, VPN Gate, IPIDEA Proxy, BigMama Proxy, Space Proxies, Nexus Proxy y Proxy Rack, entre otros.

Se ha proporcionado una lista completa de indicadores asociados con esta actividad, incluyendo direcciones IP y nombres de usuario/contraseñas, que se puede acceder aquí.

Esta advertencia llega después de que Cisco alertara sobre ataques de rociado de contraseñas dirigidos a servicios de VPN de acceso remoto como parte de sus *«esfuerzos de reconocimiento»*.

Además, se informa que los actores de amenazas están explotando una vulnerabilidad ya corregida que afecta a los routers TP-Link Archer AX21 (CVE-2023-1389, puntuación CVSS: 8.8) para distribuir varias familias de malware de botnet DDoS, incluidas AGoent, Condi, Gafgyt, Mirai, Miori y MooBot.

Los investigadores de seguridad Cara Lin y Vincent Li señalan que los botnets continúan atacando de manera persistente las vulnerabilidades de IoT, y enfatizan la importancia de que los usuarios apliquen parches de seguridad de manera oportuna para proteger sus redes.