🔐 Análisis Educativo — Vulnerabilidad WPS PIN en Router Arris TG2482

⚙️ **Propósito:** Este informe documenta una investigación **educativa y ética** sobre una vulnerabilidad presente en routers **Arris TG2482** utilizados por el proveedor, con el fin de **promover la ciberseguridad y la concienciación tecnológica**.
🧪 Todas las pruebas se realizaron en un **entorno controlado y autorizado**.

📘 Introducción

Durante una auditoría de laboratorio, se identificó una debilidad en la función **WPS (Wi-Fi Protected Setup)** del router Arris TG2482.
Este mecanismo, diseñado para facilitar la conexión de dispositivos a la red inalámbrica mediante un PIN o un botón físico, **puede ser manipulado** por atacantes si no se configura adecuadamente.

El estudio se realizó con fines **educativos y de investigación en ciberseguridad**, sin fines maliciosos ni acceso a redes de terceros.

🧩 ¿Qué es WPS y por qué es vulnerable?

Elemento	Descripción
🧠 **WPS (Wi-Fi Protected Setup)**	Permite conectar dispositivos al Wi-Fi con un PIN o un botón físico.
⚠️ **El problema**	El PIN de 8 dígitos se valida en dos mitades (4+3), reduciendo la complejidad del ataque.
🔓 **Pixie-Dust Attack**	Aprovecha una debilidad criptográfica del chip del router para obtener el PIN sin fuerza bruta completa.
💡 **Resultado**	En ciertos firmwares del mercado, el router revela el PIN y la contraseña Wi-Fi en minutos si WPS está activado.

🧠 Evidencia de laboratorio

📸 Durante las pruebas controladas se utilizó un entorno aislado para verificar la vulnerabilidad.
En los registros técnicos se observó:

- WPS habilitado por defecto en el router TG2482.

- PIN WPS obtenido mediante ataque **Pixie-Dust** en pocos minutos.
- Confirmación de recuperación del **PSK (contraseña Wi-Fi)**.

🔒 Todos los datos sensibles (SSID, BSSID, contraseñas) fueron **enmascarados** para preservar la privacidad.

⚙️ Análisis técnico simplificado

- El protocolo WPS se basa en intercambiar claves generadas por un **algoritmo pseudoaleatorio (PRNG)**.
- En algunos modelos Arris, este PRNG no es lo suficientemente aleatorio.
- Un atacante puede calcular el PIN WPS y derivar la contraseña sin necesidad de múltiples intentos.
- Esto se conoce como **ataque Pixie-Dust**, documentado desde 2014.

💬 En resumen: si tu router tiene WPS activado, es como dejar una "puerta lateral" abierta a tu red Wi-Fi.

💥 Impacto potencial

Nivel	Riesgo	Descripción
🧍 Usuario doméstico	Medio	Alguien cercano podría conectarse sin permiso.
🏢 Empresas	Alto	Posible acceso a información interna o ataques MITM.
🌐 General	Crítico	Vulnerabilidad persistente si no se actualiza el firmware.

🛡️ Recomendaciones

Para usuarios

✅ **Desactivar WPS:**
Entra en 192.168.0.1 o 192.168.100.1 → Configuración inalámbrica → Desactiva *WPS*.

✅ **Actualizar el firmware:**
Contacta a **tu proveedor** o descarga actualizaciones desde Arris Support.

✅ **Usar WPA2 o WPA3:**
Evita WEP o WPA antiguo.

✅ **Cambiar contraseñas por defecto:**
Usa una clave larga y compleja, y cambia también las credenciales del panel de administración.

✅ **Revisar conexiones activas:**
Accede al panel del router y elimina dispositivos no reconocidos.

Para técnicos y administradores

🧩 **Aplicar políticas seguras de red:** segmentar Wi-Fi de invitados, IoT y administración.
🧩 **Auditar equipos periódicamente:** comprobar logs, actualizaciones y estados de WPS.
🧩 **Reportar vulnerabilidades:** informar a fabricantes o ISPs de posibles fallos encontrados.

🧪 Metodología de prueba

1. Creación de entorno aislado (sin acceso a redes reales).
2. Autorización expresa del propietario del equipo.
3. Auditoría del protocolo WPS con herramientas legales y documentadas.
4. Registro de resultados y documentación educativa.
5. Eliminación de datos sensibles al finalizar las pruebas.

🖇️ Todas las acciones se realizaron siguiendo principios de **ética hacker** y **divulgación responsable**.

📚 Conclusiones

La función WPS, aunque práctica, **no es segura en muchos dispositivos antiguos**.
La investigación demuestra que los routers Arris TG2482 (firmware) pueden ser vulnerables si esta función permanece habilitada.

💡 **Solución práctica:** desactivar WPS, mantener el firmware actualizado y usar estándares modernos de seguridad inalámbrica (WPA2/WPA3).

🔗 Referencias

- CERT Vulnerability Note VU#723755 — WPS brute-force
- Pixie-Dust Attack — Dominique Bongard, 2014 (USENIX)
- Arris Official Support

📜 Nota final

Este documento tiene **fines educativos y de concienciación en ciberseguridad**.
No se promueve el uso indebido de la información aquí expuesta.

No me hago responsable del uso que le puedan dar, esto solo es informativo.
Realiza auditorías **solo en equipos propios o con autorización explícita**.