BOLETÍN DE ALERTA

Boletín Nro.: 2023-28
Fecha de publicación: 01/06/2023

Tema: Explotación activa de vulnerabilidad en Router Ruckus Wireless.

Algunos de los productos afectados son:

- RUCKUS H350.
- RUCKUS H550.
- RUCKUS R350.
- RUCKUS T350c.
- RUCKUS T350d.
- RUCKUS T350se.
- RUCKUS T811-CM (Non-SFP).

Se puede acceder al listado completo de productos afectados aquí.

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad explotada activamente que afecta a Router Ruckus Wireless, que permitiría a un atacante realizar ataques del tipo *server-side request forgery* (*SSRF*), ejecución remota de código (*RCE*), entre otros. Actualmente para el CVE-2023-25717 existe prueba de concepto (*PoC*) pública.

La vulnerabilidad identificada como CVE-2023-25717, de severidad "Crítica" y con puntuación asignada de 9.8. Esta vulnerabilidad explotada activamente se debe al manejo inadecuado de las solicitudes *HTTP* en el proceso de inicio de sesión de la interfaz web de administración en Ruckus Wireless. Esto permitiría a un atacante no autenticado a través de una solicitud *HTTP GET* especialmente diseñada, realizar ataques del tipo *server-side request forgery* (*SSRF*), c*ross-site request forgery* (*CSRF*), ejecución remota de código (*RCE*) y tomar el control de los dispositivos de punto de acceso inalámbrico (*AP*) afectados.

Impacto:

La explotación exitosa de esta vulnerabilidad podría permitir a un atacante realizar ataques del tipo *server-side request forgery* (*SSRF*), c*ross-site request forgery* (*CSRF*), ejecución remota de código (*RCE*) y potencialmente comprometer totalmente los dispositivos afectados.

Solución:

Recomendamos acceder a las actualizaciones correspondientes provista por el fabricante en el siguiente enlace:

- https://support.ruckuswireless.com/security_bulletins/315

Información adicional:

- https://www.cert.gov.py/noticias/botnet-de-malware-andoryu-explota-activamente-vulnerabilidad-de-ruckus-wireless/
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://nvd.nist.gov/vuln/detail/CVE-2023-25717
- https://support.ruckuswireless.com/security_bulletins/315