BOLETÍN DE ALERTA

Boletín Nro.: 2023-27
Fecha de publicación: 25/05/2023

Tema: Vulnerabilidad de día cero (*0-day*) en Barracuda Email Security Gateway (*ESG*)

Las versiones afectadas son:

- Email Security Gateway (*ESG*), versiones 5.1.3.001 al 9.2.0.006.

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad de día cero (*0-day*) que afecta a Barracuda Email Security Gateway (*ESG*). La vulnerabilidad identificada como CVE-2023-2868, de severidad "Crítica" y con puntuación asignada de 9.4. Esta vulnerabilidad se debe a la validación incorrecta de datos de entrada en un archivo *.tar* proporcionado por el usuario de Email Security Gateway (*ESG*). Esto permitiría a un atacante remoto obtener acceso no autorizado a través del operador *qx* de Perl, realizar formateo de nombres de archivos y ejecución de comandos en el sistema afectado.

Impacto:

La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto obtener acceso no autorizado y realizar ejecución de comandos en el sistema afectado.

Solución:

El proveedor ha emitido una actualización de seguridad *BNSF-36456* de instalación automática, para más información ver el siguiente enlace. La investigación sobre dicha vulnerabilidad se limitó al producto Email Security Gateway (ESG) y no al entorno específico del cliente. Por lo tanto, los clientes afectados deben verificar sus entornos y determinar cualquier acción adicional que deseen realizar.

Adicionalmente recomendamos estar pendiente a posibles actualizaciones relacionadas con la vulnerabilidad que se publiquen en el futuro en el siguiente enlace.

Información adicional:

- https://securityaffairs.com/146620/hacking/barracuda-email-security-gateway-bug.html
- https://nvd.nist.gov/vuln/detail/CVE-2023-2868
- https://status.barracuda.com/
- https://www.securityweek.com/zero-day-vulnerability-exploited-to-hack-barracuda-email-security-gateway-appliances/
- https://www.barracuda.com/company/legal/esg-vulnerability
- https://campus.barracuda.com/product/emailsecuritygateway/doc/11141920/release-notes/