BOLETÍN DE ALERTA

Boletín Nro.: 2023-27
Fecha de publicación: 25/05/2023
Fecha de actualización: 09/06/2023

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

Actualizaciones:

- **09/06/2023:** Se han lanzado recomendaciones para reemplazar los dispositivos *ESG* afectados por la vulnerabilidad de Día Cero además de las publicaciones de *IOCs* de posibles compromisos.

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.

Así también se han identificado varios *malware* (*SALTWATER, SEASPY y SEASIDE*) que están explotando esta vulnerabilidad en un subconjunto de dispositivos que permiten dar un acceso persistente a los atacantes, a través de backdoor.

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.

Recomendaciones:

- Reemplazar de inmediato los dispositivos Email Security Gateway (*ESG*) afectados, independientemente del nivel de versión del parche. Si no ha reemplazado su dispositivo después de recibir un aviso en su interfaz de usuario, comuníquese con soporte (support@barracuda.com).
- Adicionalmente, el equipo de seguridad de Barracuda recomienda rotar (cambiar) todas las credenciales aplicables conectadas al dispositivo Email Security Gateway (*ESG*) afectado:
    - Servidores *LDAP/AD.*
    - Barracuda Cloud Control.
    - Servidores *FTP.*
    - *SMB.*
    - Certificados *TLS* privados.
- Revisar los registros de red para cualquiera de los *IOC* enumerados a continuación y cualquier dirección *IP* desconocida. Contactar con compliance@barracuda.com si se identifica alguno de los mencionados.

Para visualizar los indicadores de compromiso IOCs (*Endpoint IOCs, Network IOCs, YARA Rules*) ver el siguiente enlace.

Información adicional:

- https://www.cert.gov.py/wp-content/uploads/2023/05/BOL-CERT-PY-2023-27-Vulnerabilidad-de-dia-cero-0-day-en-Barracuda-Email-Security-Gateway-ESG.pdf
- 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/
- https://www.barracuda.com/company/legal/esg-vulnerability