BOLETÍN DE ALERTA

Boletín Nro.: 2023-57
Fecha de publicación: 27/12/2023
Tema: Vulnerabilidad en Email Security Gateway Barracuda

Productos afectados:

- Versiones del firmware del Barracuda ESG Appliance 5.1.3.001 hasta 9.2.1.001.
- Versión del Spreadsheet::ParseExcel 0.65.

Descripción:

Se ha reportado una vulnerabilidad en una librería de terceros en Barracuda ESG Appliance que permite la inyección de parámetros. La vulnerabilidad está identificada como CVE-2023-7102. La vulnerabilidad de la librería o módulo Spreadsheet::ParseExcel permite la ejecución de código arbitrario (ACE) debido a la inserción de una entrada no validada desde un archivo de tipo de cadena. La severidad para ambos aún no está definida a la fecha.

Impacto:

Un actor malicioso podría inyectar y ejecutar código arbitrario explotando esta vulnerabilidad. Actualmente existe una Prueba de Concepto (PoC) publicada.

Solución:

Se recomienda verificar la última actualización del firmware.

Información adicional:

- https://nvd.nist.gov/vuln/detail/CVE-2023-7102
- https://www.barracuda.com/company/legal/esg-vulnerability
- https://www.cve.org/CVERecord?id=CVE-2023-7101
- https://www.cve.org/CVERecord?id=CVE-2023-7102