
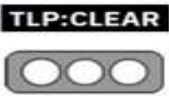


Nro. Alerta:	AL-2023-023	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	05-jun-2023	<b>Vulnerabilidad de día cero en dispositivos de seguridad de correo electrónico Barracuda</b>	V 1.1

### 1. DATOS GENERALES:

**Clase de alerta:** Vulnerabilidad  
**Tipo de incidente:** Explotación de vulneraciones conocidas  
**Nivel de riesgo:** Medio

### 2. ALERTA

Se ha detectado una vulnerabilidad crítica de inyección de comando remoto con puntuación de 9.4 que afecta solo a los dispositivos físicos Barracuda Email Security Gateway (CVE-2023-2868).





Figura 1.- Fabricante de soluciones de Email Security Gateway  
 Fuente: <https://www.helpnetsecurity.com/2023/05/30/barracuda-esg-zero-day/>

### 3. INTRODUCCIÓN

El 19 de mayo de 2023, el fabricante de soluciones de Email Security Gateway (ESG) Barracuda, en respuesta a la vulnerabilidad identificada con código CVE-2023-2868; libero y aplicó un parche de seguridad (BNSF-36456) a todos los dispositivos Email Security Gateway versiones 5.1.3.001 – 9.2.0.006 de forma masiva.



Nro. Alerta:	AL-2023-023	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	05-jun-2023	<b>Vulnerabilidad de día cero en dispositivos de seguridad de correo electrónico Barracuda</b>	V 1.1

Los usuarios cuyos dispositivos se vieron afectados, recibieron del fabricante las notificaciones a través de la interfaz de usuario de ESG sobre las acciones a tomar.



El resultado de la investigación que aun esta en curso por parte del fabricante y expertos contratados, es el siguiente:

- La vulnerabilidad existía en un módulo que inicialmente analiza los archivos adjuntos de los correos electrónicos entrantes. Ningún otro producto de Barracuda, incluidos servicios de seguridad de correo electrónico SaaS, estuvo sujeto a la vulnerabilidad identificada.
- La evidencia más temprana identificada de explotación de CVE-2023-2868 es de octubre de 2022.
- Se identificó malware en un subconjunto de dispositivos que permiten el acceso persistente de puerta trasera.
- Se identificó evidencia de ex filtración de datos en un subconjunto de dispositivos afectados.
- Los usuarios afectados han sido notificados a través de la interfaz de usuario de ESG sobre las acciones que deben tomar.

Con la ayuda de expertos en seguridad cibernética, se descubrió que se habían lanzado al menos tres cargas maliciosas diferentes en los dispositivos afectados:

1. SALTWATER (AGUA SALADA), un módulo troyano para el demonio Barracuda SMTP (bsmtpd), que sirve como una puerta trasera que tiene capacidades de proxy y tunelización y permite a los atacantes cargar o descargar archivos arbitrarios y ejecutar comandos.
2. SEASPY, una puerta trasera de persistencia utilizando el formato x64 ELF, que se hace pasar por un servicio legítimo de Barracuda Networks y se establece como un filtro PCAP, específicamente monitoreando el tráfico en el puerto 25 (SMTP) y el puerto 587.



Nro. Alerta:	AL-2023-023	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	05-jun-2023	<b>Vulnerabilidad de día cero en dispositivos de seguridad de correo electrónico Barracuda</b>	V 1.1

- SEASIDE (PLAYA), un módulo basado en el Lenguaje de Programación de secuencia de comandos Lua para el demonio Barracuda SMTP (bsmtpd), que establece una conexión con el servidor C2 de los atacantes y ayuda a establecer un shell inverso (para brindar acceso al sistema).

El fabricante indica que su investigación se limita a su producto Email Security Gateway, por lo que depende de los clientes revisar sus entornos y determinar cualquier acción adicional que requiera adoptar.



Como apoyo para sus clientes, el fabricante ha desarrollado una serie de reglas YARA que se pueden encontrar en la página del fabricante como apoyo en la detección.

### Cronología del evento

- El 18 de mayo de 2023, se alertó al fabricante sobre un tráfico anómalo procedente de los dispositivos Barracuda Email Security Gateway (ESG).
- El 18 de mayo de 2023, el fabricante contrató a expertos en seguridad cibernética, para ayudar en la investigación.
- El 19 de mayo de 2023, el fabricante identificó una vulnerabilidad (CVE-2023-2868) en dispositivos Email Security Gateway (ESG).
- El 20 de mayo de 2023, se aplicó un parche de seguridad para remediar la vulnerabilidad a todos los dispositivos ESG.
- El 21 de mayo de 2023, se implementó un script en todos los dispositivos afectados para contener el incidente y contrarrestar los métodos de acceso no autorizados.

A partir de esta fecha se está implementando una serie de parches de seguridad en todos los dispositivos por parte del fabricante.



Nro. Alerta:	AL-2023-023	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	05-jun-2023	<b>Vulnerabilidad de día cero en dispositivos de seguridad de correo electrónico Barracuda</b>	V 1.1

#### 4. VECTOR DE ATAQUE:

La vulnerabilidad provino de una validación de entrada incompleta de los archivos .tar proporcionados por el usuario en lo que respecta a los nombres de los archivos contenidos en el archivo. En consecuencia, un atacante remoto podría formatear los nombres de los archivos de una manera particular que daría lugar a la ejecución remota de un comando del sistema a través del operador qx del lenguaje de Programación Perl con los privilegios del producto Email Security Gateway.

La investigación de Barracuda hasta la fecha ha determinado que un tercero utilizó la técnica descrita anteriormente para obtener acceso no autorizado a un subconjunto de dispositivos ESG.

#### 5. INDICADORES DE COMPROMISO:

Los indicadores de compromiso de las tres cargas maliciosas en los dispositivos afectados son:


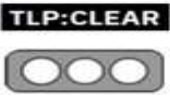
##### SALTWATER (AGUA SALADA),

**Identificado en la ruta:** /home/product/code/firmware/current/lib/smtp/modules en un subconjunto de dispositivos ESG.

**Metadatos** del archivo relacionados con una variante de AGUA SALADA:

Nombre	SHA256	
mod_udp.so	1c6cad0ed66cf8fd438974e1eac0bc6dd9119f84892930cb71cb56a5e985f0a4	
MD5	Tipo de archivo	Tamaño (bytes)
827d507aa3bde0ef903ca5dic60cdec8	ONCE x86	1,879,643



Nro. Alerta:	AL-2023-023	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	05-jun-2023	<b>Vulnerabilidad de día cero en dispositivos de seguridad de correo electrónico Barracuda</b>	V 1.1

**SEASPY.**

**Identificado en la ruta:** /sbin/ en un subconjunto de dispositivos ESG.  
**Metadatos** del archivo relacionados con una variante de SEASPY.

Nombre	SHA256	
BarracudaMailService	3f26a13f023ad0dcd7f2aa4e7771bba74910ee227b4b36ff72edc5f07336f115	
MD5	Tipo de archivo	Tamaño (bytes)
4ca4f582418b2cc0626700511a6315c0	ELFO x64	2,924,217

**SEASIDE (PLAYA).**

**Metadatos** del archivo relacionados con SEASIDE.



Nombre	SHA256	
mod_require_helo.lua	fa8996766ae347ddcbbd1818fe3a878272653601a347d76ea3d5dfc227cd0bc8	
MD5	Tipo de archivo	Tamaño (bytes)
cd2813f0260d63ad5adf0446253c2172	tomar módulos	2,724

**IOC DE PUNTO FINAL**

A continuación se enumera los IOC de puntos finales, incluido el malware y las utilidades, atribuidos a la actividad del atacante durante la investigación.

	Nombre del archivo	Hachis MD5	Tipo
1	appcheck.sh	N / A	guion bash
2	aacore.sh	N / A	guion bash



Nro. Alerta:	AL-2023-023	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	05-jun-2023	<b>Vulnerabilidad de día cero en dispositivos de seguridad de correo electrónico Barracuda</b>	V 1.1



3	1.sh	N / A	guion bash
4	mod_udp.so	827d507aa3bde0ef903ca5dic60cdec8	Variante AGUA SALADA
5	intención	N / A	N / A
6	install_helo.tar	2ccb9759800154de817bf779a52d48f8	Paquete TAR
7	intento_hola	f5ab04a920302931a8bd063f27b745cc	guion bash
8	p.d.	177add288b289d43236d2dba33e65956	Concha inversa
9	update_v31.sh	881b7846f8384c12c7481b23011d8e45	guion bash
10	mod_require_helo.lua	cd2813f0260d63ad5adf0446253c2172	PLAYA
11	BarracudaMailService	82eaf69de710abdc5dea7cd5cb56cf04	SEASPY
12	BarracudaMailService	e80a85250263d58cc1a1dc39d6cf3942	SEASPY
13	BarracudaMailService	5d6cba7909980a7b424b133fbac634ac	SEASPY
14	BarracudaMailService	1bbb32610599d70397adfdaf56109ff3	SEASPY
15	BarracudaMailService	4b511567cfa8dbaa32e11baf3268f074	SEASPY
16	BarracudaMailService	a08a99e5224e1baf569fda816c991045	SEASPY
17	BarracudaMailService	19ebfe05040a8508467f9415c8378f32	SEASPY
18	mod_udp.so	1fea55b7c9d13d822a64b2370d015da7	Variante AGUA SALADA
19	mod_udp.so	64c690f175a2d2fe38d3d7c0d0ddb6e	Variante AGUA SALADA
20	mod_udp.so	4cd0f3219e98ac2e9021b06af70ed643	Variante AGUA SALADA

**Tabla 1.- Indicadores de compromiso de Punto final**  
 Fuente: <https://www.barracuda.com/company/legal/esq-vulnerability>

A continuación, se enumera los IOC de la red, incluidas las direcciones IP y los nombres de dominio, atribuidos a la actividad del atacante durante la investigación:

	Indicador	ADN	Ubicación
1	xxl17z.dnslog.cn	N / A	N / A
2	mx01.bestfindthetruth.com	N / A	N / A
3	64.176.7.59	AS-CHOOPA	A NOSOTROS
4	64.176.4.234	AS-CHOOPA	A NOSOTROS
5	52.23.241.105	AMAZON-AES	A NOSOTROS
6	23.224.42.5	CloudRadium LLC	A NOSOTROS
7	192.74.254.229	PEG TECH INC	A NOSOTROS
8	192.74.226.142	PEG TECH INC	A NOSOTROS
9	155.94.160.72	QuadraNet Enterprises LLC	A NOSOTROS
10	139.84.227.9	AS-CHOOPA	A NOSOTROS
11	137.175.60.253	PEG TECH INC	A NOSOTROS
12	137.175.53.170	PEG TECH INC	A NOSOTROS
13	137.175.51.147	PEG TECH INC	A NOSOTROS



Nro. Alerta:	AL-2023-023	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	05-jun-2023	<b>Vulnerabilidad de día cero en dispositivos de seguridad de correo electrónico Barracuda</b>	V 1.1

14	137.175.30.36	PEG TECH INC	A NOSOTROS
15	137.175.28.251	PEG TECH INC	A NOSOTROS
16	137.175.19.25	PEG TECH INC	A NOSOTROS
17	107.148.219.227	PEG TECH INC	A NOSOTROS
18	107.148.219.55	PEG TECH INC	A NOSOTROS
19	107.148.219.54	PEG TECH INC	A NOSOTROS
20	107.148.219.53	PEG TECH INC	A NOSOTROS
21	107.148.219.227	PEG TECH INC	A NOSOTROS
22	107.148.149.156	PEG TECH INC	A NOSOTROS
23	104.223.20.222	QuadraNet Enterprises LLC	A NOSOTROS
24	103.93.78.142	EDGENAP LTD	JP
25	103.27.108.62	TOPWAY GLOBAL LIMITADA	Hong Kong
26	137.175.30.86	PEGTECHINC	A NOSOTROS
27	199.247.23.80	AS-CHOOPA	DE
28	38.54.1.82	KAOPU NUBE HK LIMITADA	SG
29	107.148.223.196	PEGTECHINC	A NOSOTROS
30	23.224.42.29	CNSERVERS	A NOSOTROS
31	137.175.53.17	PEGTECHINC	A NOSOTROS
32	103.146.179.101	BANCO GIGABIT MUNDIAL	Hong Kong

Tabla 2.- Indicadores de compromiso de red



Fuente: <https://www.barracuda.com/company/legal/esg-vulnerability>

## 6. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Realizar las actualizaciones sugeridas por el fabricante.
- Use el principio de privilegio mínimo en la gestión de usuario de las plataformas tecnológicas.
- Implemente la segmentación de la red para que, si un sistema está infectado, pueda aislarse fácilmente y evitar que el código malicioso se propague por la red.
- Realice copias de seguridad frecuentes de la configuración de los equipos.
- Frente a la detección de un incidente, cambie las contraseñas de todos los componentes de red.



Nro. Alerta:	AL-2023-023	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	05-jun-2023	<b>Vulnerabilidad de día cero en dispositivos de seguridad de correo electrónico Barracuda</b>	V 1.1

- Revise los registros de red y busque IOC e IP compartidas por el fabricante para el respectivo monitoreo y/o bloqueo.
- Utilice las reglas YARA para buscar el archivo TAR malicioso que explota CVE-2023-2868 sugeridas por el fabricante.

## 7. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

## 8. REFERENCIAS:

Barracuda. (01 de 06 de 2023). *Barracuda*. Obtenido de <https://www.barracuda.com/company/legal/esg-vulnerability>

Barracuda. (30 de 05 de 2023). *Barracuda*. Obtenido de <https://status.barracuda.com/incidents/34kx82j5n4q9>

Corporation, T. M. (s.f.). *CVE*. Obtenido de <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-2868>

Zorz, Z. (30 de 05 de 2023). *Help Net Security*. Obtenido de <https://www.helpnetsecurity.com/2023/05/30/barracuda-esg-zero-day/>

