GammaCSOC-CERT
By Gamma Ingenieros



GAMMA INGENIEROS

ALERTA TEMPRANA

OpenSSH en Alpine Linux: acceso sin contraseña

6 de noviembre de 2026

ALERTA TEMPRANA DE CIBERSEGURIDAD

Gamma CSOC-CERT emite esta alerta para que directivos, áreas de negocio y equipos técnicos tomen acción frente a una falla en el servicio de acceso remoto OpenSSH cuando corre sobre Alpine Linux y otros sistemas Linux con la biblioteca musl y sin PAM. El documento está escrito para lectores no técnicos; la sección 6.2 contiene las instrucciones para quienes administran servidores.

Nivel de alerta	**ALTO** **Prioridad 1**
Qué está afectado	El servidor OpenSSH (sshd) anterior a la versión 10.6p2 en Linux con biblioteca musl y sin PAM. El caso principal es **Alpine Linux**, muy usado en servidores livianos, equipos de red, imágenes en la nube y algunos contenedores.
Tipo de amenaza	Omisión de la autenticación: un atacante que alcance el puerto SSH puede entrar a una cuenta sin conocer la contraseña.
Identificadores	CVE-2026-123158
Severidad oficial	Alta. 8,1 sobre 10 (CVSS v3.1, asignada por MITRE en NVD). Alpine Linux califica la falla como explotable en una sola conexión y sin reintentos.
Estado	Corrección disponible desde el 5 de noviembre de 2026 (OpenSSH 10.6p2 y paquetes corregidos de Alpine). Existen pruebas de concepto públicas. No figura en el catálogo CISA KEV a la fecha.
Acción requerida	**Actualizar openssh y reiniciar sshd hoy.** Si no es posible, deshabilitar el ingreso por contraseña.
Fuentes	NVD, proyecto OpenSSH (notas de la versión 10.6p2), aviso de seguridad de Alpine Linux.
Contacto Gamma CSOC-CERT	601 488 00 58 · +57 320 305 4929 · monitoreosoc@gammaingenieros.com

1. RESUMEN EN PALABRAS SIMPLES

SSH es la puerta que usan los administradores para entrar de forma remota a servidores y equipos. OpenSSH es el programa más usado para abrir esa puerta.

GAMMA INGENIEROS
FIRST Improving Security Together
CERT
Authorized to Use CERT™
CERT is a mark owned by
Carnegie Mellon University

El 5 de noviembre de 2026 el proyecto OpenSSH y Alpine Linux publicaron la corrección de una falla que permite entrar sin contraseña. Basta con conocer el nombre de una cuenta que no tenga contraseña asignada (algo normal en cuentas que solo entran con llave) y enviar una contraseña muy larga, de 257 a 1024 caracteres. Si en el equipo existe al menos otra cuenta con contraseña, la entrada se acepta.

Por qué es urgente: el ataque funciona en un solo intento, no deja rastro de fuerza bruta y ya hay pruebas de concepto públicas. La configuración por defecto de Alpine (ingreso por contraseña habilitado) es la configuración vulnerable.

2. QUÉ PUEDE PASAR SI NO SE ACTÚA

- **Toma de control del servidor:** si la cuenta comprometida puede elevar privilegios (por ejemplo con doas), el atacante llega a administrador.
- **Robo o filtración de información:** acceso a datos de clientes, empleados o datos personales protegidos por la Ley 1581 de 2012.
- **Puerta de entrada a la red interna:** un servidor o equipo de borde comprometido sirve para moverse hacia otros sistemas.
- **Instalación de software malicioso:** ransomware, minería de criptomonedas o uso del equipo para atacar a terceros.

3. ¿ESTOY EXPUESTO?

Para áreas no técnicas: tres preguntas

1. ¿La organización tiene servidores, máquinas virtuales en la nube o equipos de red que usen Alpine Linux?
2. ¿Alguno permite acceso remoto por SSH desde internet o desde redes de terceros?
3. ¿Quién los administra: el equipo interno, un proveedor de nube o un tercero?

Para equipos técnicos: condiciones y versiones

Un equipo está afectado si cumple **todas** estas condiciones: usa openssh-server de Alpine (sin PAM) u openssh-server-pam con UsePAM no; tiene PasswordAuthentication yes (valor por defecto); tiene una cuenta con campo de contraseña "*" (root en la imagen base desde Alpine 3.16, usuarios solo con llave, usuarios de directorio vía musl-nscd o el usuario alpine de las imágenes tiny-cloud); y tiene al menos una cuenta local con hash 5 o 6.

GAMMA INGENIEROS
FIRST Improving Security Together
CERT
Authorized to Use CERT™
CERT is a mark owned by
Carnegie Mellon University

Rama de Alpine	Versión corregida de openssh	Qué hacer
edge	10.6_p2-r0	Actualizar y reiniciar sshd.
3.24	10.3_p1-r2 (Alpine 3.24.4)	Actualizar y reiniciar sshd.
3.23	10.2_p1-r1 (Alpine 3.23.8)	Actualizar y reiniciar sshd.
3.22	10.0_p1-r11 (Alpine 3.22.8)	Actualizar y reiniciar sshd.
3.21	9.9_p2-r1 (Alpine 3.21.10)	Actualizar. Rama sin soporte desde el 1 de noviembre de 2026: planear migración.
3.16 a 3.20	3.20: 9.7_p1-r6 · 3.19: 9.6_p1-r3 · 3.18: 9.3_p2-r4 · 3.17: 9.1_p1-r7 · 3.16: 9.0_p1-r6	Actualizar y planear migración a una rama con soporte.
Otras distribuciones con musl y sin PAM	OpenSSH 10.6p2	Confirmar con el proveedor de la distribución o del equipo.

No están afectados: contenedores que no ejecutan sshd, equipos con PasswordAuthentication no, openssh-server-pam con UsePAM yes, cuentas bloqueadas con "!" e imágenes en la nube configuradas con cloud-init. Las distribuciones con glibc y PAM (Debian, Ubuntu, Red Hat y similares) no aparecen como afectadas en las fuentes consultadas.

4. LA FALLA EXPLICADA

Identificador	Qué es	Explicado en simple
CVE-2026-123158	Omisión de la autenticación por contraseña en sshd cuando se compila sin PAM y usa la biblioteca musl. La función crypt() de musl devuelve "*" como error ante claves de más de 256 bytes, y ese valor coincide con el campo de las cuentas sin contraseña.	El sistema compara la contraseña enviada con la guardada. Con una contraseña muy larga, el resultado del error es igual a lo que tienen guardado las cuentas sin contraseña, y el sistema cree que coinciden.

5. CRONOLOGÍA

Fecha	Hecho
5 nov 2026	OpenSSH publica la versión 10.6p2 con la corrección. Alpine Linux publica aviso de seguridad y paquetes corregidos para las ramas 3.16 a edge.
5 nov 2026	Se publica CVE-2026-123158 en NVD con severidad 8,1 asignada por MITRE. NVD enlaza pruebas de concepto públicas.
6 nov 2026	Gamma CSOC-CERT emite esta alerta. La falla no figura en el catálogo CISA KEV a la fecha.

6. RECOMENDACIONES

6.1 Para directivos y áreas no técnicas

1. **Confirmar hoy** con el área de tecnología o el proveedor si la organización usa Alpine Linux y en qué equipos.
2. **Priorizar** los equipos con acceso SSH desde internet o desde redes de terceros.
3. **Pedir evidencia escrita** de la actualización o de la desactivación del ingreso por contraseña, incluso a proveedores que administren los equipos.

6.2 Para equipos técnicos

A. Corregir (única solución completa)

- **Actualizar** con apk upgrade -U -a hasta las versiones de la tabla de la sección 3, o a OpenSSH 10.6p2 en otras distribuciones con musl.
- **Reiniciar sshd** (rc-service sshd restart). Actualizar el paquete no reemplaza el proceso que ya está corriendo.
- Reconstruir las imágenes base y de nube a partir de Alpine 3.21.10, 3.22.8, 3.23.8 o 3.24.4 o posteriores.

B. Si no puede actualizar hoy: medida temporal

> **Deshabilitar el ingreso por contraseña cierra el problema.** Antes, confirme que el acceso con llave funciona y mantenga abierta la sesión actual hasta probar un ingreso nuevo.

GAMMA INGENIEROS
FIRST Improving Security Together
CERT
Authorized to Use CERT™
CERT is a mark owned by Carnegie Mellon University

- Configurar **PasswordAuthentication no** en /etc/ssh/sshd_config y en un archivo de /etc/ssh/sshd_config.d (Alpine 3.19 en adelante), incluidos los bloques Match.
- Validar con sshd -t, reiniciar sshd y confirmar con sshd -T que el valor efectivo es no.

C. Proteger y vigilar

- Restringir el puerto SSH a redes de administración o VPN; no exponerlo a internet.
- Revisar las imágenes tiny-cloud de Alpine 3.18.11 a 3.24.3: traen el usuario alpine sin contraseña y con doas sin contraseña.
- Bloquear con "!" las cuentas que no deben iniciar sesión.

D. Si sospecha un ataque

- Buscar en /var/log/messages líneas de sshd "Accepted password" para cuentas sin contraseña (alpine, root o usuarios solo con llave).
- Revisar uso de doas, usuarios creados, archivos y llaves autorizadas recientes.
- Si no puede descartar un ingreso, trate el equipo como comprometido, aíslelo, preserve evidencia y contacte a Gamma CSOC-CERT.

7. CONCLUSIONES

1. **El riesgo es alto y actual.** No exige contraseña, funciona en un solo intento y hay pruebas de concepto públicas.
2. **La exposición depende de la configuración.** Alpine con ingreso por contraseña habilitado, que es el valor por defecto, está afectado.
3. **La solución completa es actualizar y reiniciar sshd.** Deshabilitar el ingreso por contraseña es la alternativa inmediata.
4. **SSH no debe estar expuesto a internet.** Limitarlo a redes de administración reduce este y futuros riesgos.

Gamma CSOC-CERT · By Gamma Ingenieros. Esta alerta se basa en información pública disponible al 6 de noviembre de 2026 y puede cambiar a medida que se conozcan nuevos detalles.

GAMMA INGENIEROS
FIRST Improving Security Together
CERT
Authorized to Use CERT™
CERT is a mark owned by Carnegie Mellon University

8. GLOSARIO

Término	Significado
SSH / sshd	Protocolo de acceso remoto seguro a servidores. sshd es el programa servidor que recibe las conexiones.
Alpine Linux	Distribución de Linux liviana, usada en servidores, nube, contenedores y equipos de red.
musl	Biblioteca base de funciones del sistema que usa Alpine en lugar de la más común, glibc.
PAM	Módulo que gestiona la autenticación en Linux. Con PAM activo esta falla no aplica.
Hash de contraseña	Forma cifrada en que el sistema guarda una contraseña.
doas	Herramienta que permite a un usuario ejecutar comandos como administrador.
Prueba de concepto	Código público que demuestra cómo aprovechar una falla.
CVE	Código único con el que se identifica públicamente una vulnerabilidad.
CVSS	Escala de 0 a 10 para medir la severidad técnica de una vulnerabilidad.
TLP:CLEAR	Esta información se puede compartir sin restricción.

9. REFERENCIAS

- NVD, CVE-2026-123158: https://nvd.nist.gov/vuln/detail/CVE-2026-123158
- OpenSSH, notas de la versión 10.6p2: https://www.openssh.org/releasenotes.html#10.6p2
- Alpine Linux, aviso de seguridad openssh-server: https://alpinelinux.org/posts/2026-11-05-openssh-password-authentication-bypass/
- OpenSSH Portable, cambio de código de la corrección: https://github.com/openssh/openssh-portable/commit/4353fdc43ef646c43a8dda7025cc1a898caf1482