GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

18 November 2026

Advisory 383: OpenSSH Password Authentication Bypass on musl Linux "*sshole" (CVE-2026-123158).

Release Date: 11th November 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above product(s). This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-123158, nicknamed "*sshole", is a password authentication bypass in the OpenSSH server (sshd) on Linux systems built with the musl C library and without PAM, such as Alpine Linux. Accounts that should have password login disabled (shown as "*" in /etc/shadow) can be logged into remotely by sending a specially crafted password. The flaw has existed for about ten years.

What are the systems affected?

The vulnerability affects OpenSSH servers before 10.6p2 on musl-based Linux without PAM, including:

- Alpine Linux, including Alpine-based Docker and container images
- OpenWrt routers and other embedded devices built with Buildroot or Yocto
- Network appliances and IoT devices that run sshd on musl
- Standard glibc distributions with PAM, such as Debian, Ubuntu and Red Hat, are not affected in their default configuration

Not affected / patched version:

- OpenSSH 10.6p2 or later
- Alpine fixed openssh packages, for example edge 10.6_p2-r0 and the fixes in Alpine 3.21.10, 3.22.8, 3.23.8 and 3.24.4

What does this mean?

Successful exploitation may allow attackers to:

- Log in over SSH to accounts that should not accept passwords
- Take control of servers, containers, routers and embedded devices
- Install malware, botnet agents or cryptominers
- Use compromised devices to attack other systems

Mitigation process

CERTVU recommends the following:

1. Update OpenSSH and restart sshd
Update to OpenSSH 10.6p2 or your distribution's fixed package (on Alpine, apk upgrade openssh), then restart sshd. The fix does not take effect until sshd restarts. Rebuild container images from updated base images.

2. Disable password authentication if you cannot update
3. Restrict SSH access
4. Check for compromise

Report suspected compromise to CERTVU at incident@cert.gov.vu.

Reference

1. https://www.openssh.org/releasenotes.html#10.6p2
2. https://alpinelinux.org/posts/2026-11-05-openssh-password-authentication-bypass/
3. https://www.cve.org/CVERecord?id=CVE-2026-123158
4. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-123158