OpenSSH Release Notes

Overview and Key Changes

November 5, 2026 | Prepared by Adi Bleih | Covers OpenSSH 9.8 through 10.6p2

Executive Summary

OpenSSH 10.6p2 shipped on November 5, 2026. It closes a critical password authentication bypass on some Linux systems. If you run sshd on musl-based Linux with pluggable authentication modules (PAM) disabled, upgrade today.

CHECK POINT FINDING	**New Check Point findings.** Our testing adds two points to the public advisory. First, the attack needs a second account that is active and has a real password. A stored hash alone is not enough. Second, two conditions are visible remotely, before login: the OpenSSH version in the SSH banner, and whether the server accepts password authentication. Servers that don't offer passwords are not exposed.

OpenSSH is the standard Secure Shell (SSH) implementation on Linux, BSD, and macOS. It includes the ssh client, the sshd server, scp, sftp, ssh-agent, and ssh-keygen. The release notes page lists every release, newest first.

Three trends define the 2025–2026 releases:

- **Fixes arrive faster.** Since 10.5, the OpenSSH team ships fixes as they land. AI tools now find many bugs, and other researchers often find the same ones later. Attackers likely can too
- **Post-quantum is the default.** Hybrid post-quantum key exchange is on by default since 10.0. A post-quantum signature algorithm joined it in 10.6
- **Hardening never stops.** Every release removes weak crypto, shrinks the pre-authentication attack surface, and tightens input checks. Some old configurations break along the way

Recent Releases

Five releases shipped in 2026, and four of them came after July. That's the faster release policy at work.

Release	Date	What changed
10.6p2	November 5, 2026	Fixes a critical password authentication bypass (musl libc, PAM disabled); accepts the ML-DSA hybrid as a CA signature
10.6	October 6, 2026	Fixes a compression side channel and sftp path checks; enables post-quantum signatures; starts deprecating scp -R
10.5	August 11, 2026	Fixes an ssh-agent lock bypass and a client use-after-free; requires elliptic-curve cryptography (ECC) in libcrypto
10.4	July 6, 2026	Blocks malicious-server tricks in sftp and scp; adds experimental ML-DSA signatures; enforces stricter rekeying
10.3	April 2, 2026	Fixes certificate principal matching; hardens against shell injection; supports the IETF agent protocol
10.2	October 10, 2025	Fixes broken ControlPersist sessions
10.1	October 6, 2025	Warns on non-post-quantum key exchange; moves agent sockets to ~/.ssh/agent
10.0	April 9, 2025	Removes DSA; makes ML-KEM hybrid key exchange the default; splits out an sshd-auth binary
9.9p2	February 18, 2025	Fixes CVE-2025-26465 (man-in-the-middle with VerifyHostKeyDNS) and CVE-2025-26466 (denial of service)
9.8	July 1, 2024	Fixes a critical sshd race condition that allows root code execution; turns on PerSourcePenalties by default

Security Fixes That Matter Most

Two fixes are critical. Most others need a non-default setting or a malicious server before anyone can exploit them. Severity marked "assessed" is our own judgment where no public score was found.

Version	Part	Issue	CVE	Severity
10.6p2	sshd	Password authentication bypass on Linux with musl libc and PAM disabled, such as Alpine	None assigned yet	**Critical** assessed
10.6	ssh, sshd	Shared LZ77 compression dictionary leaks plaintext across multiplexed channels; compression is now weaker as a result	CVE-2026-110926	**Medium** CVSS 5.3, OpenCVE
10.6	sftp	A malicious server can steer a recursive copy outside the target directory	Not found	**Medium** assessed
10.6	sshd	Generic Security Services API (GSSAPI) credentials from a failed login can carry into a later successful one	CVE-2026-106555	Not scored in sources found
10.5	ssh-agent	A locked agent refuses session binding, so local-only operations can run remotely	Not found	**Medium** assessed
10.4	sftp, scp	A malicious server can drop downloaded files in unexpected places	Not found	**Medium** assessed
10.3	sshd	Certificates with empty principals match any user through authorized_keys	Not found	**Medium** assessed
9.9p2	ssh	An on-path attacker can impersonate any server when VerifyHostKeyDNS is on (off by default)	CVE-2025-26465	**High** assessed
9.8	sshd	"regreSSHion": race condition in 8.5p1–9.7p1 allows unauthenticated remote code execution as root on glibc Linux	CVE-2024-6387	**Critical** CVSS 8.1, Gatewatcher

Two fixes deserve context. The compression attack comes from Ruhr University Bochum research, the first known compression side channel against SSH. In the lowest-noise scenario, it recovers an eight-character secret in at most 276 guesses. The risk stays narrow, though: the ssh client does not offer compression by default, per Red Hat. regreSSHion, by contrast, is a regression of a 2006 bug, and Qualys counted over 14 million potentially vulnerable instances, per CyberInsider.

One pattern keeps coming back: shell injection through usernames or hostnames on the command line. These values expand inside ProxyCommand or Match exec. Releases 9.6, 10.1, 10.3, and 10.6 each tighten the filters. The OpenSSH team says no filter can be complete. Never pass untrusted input to an ssh command line.

Deep Dive: The 10.6p2 Password Bypass

> Anyone who can reach the SSH port can log in without a password. It takes one connection, works every time, and needs no retries, according to the Alpine Linux advisory.

How it works. Without PAM, sshd hashes the password attempt with crypt() and compares it to the stored field. For accounts with no salt, sshd borrows another account's salt. musl's crypt() returns * as an error when the input exceeds 256 bytes. Accounts with no password also store *. So a 257 to 1,024 byte password "matches," and the login succeeds.

Who is exposed. All of these must be true:

- sshd runs without PAM on musl-based Linux (Alpine's default openssh-server package, or openssh-server-pam with UsePAM no)
- PasswordAuthentication is yes, the OpenSSH default
- An account has * as its password field: key-only users, directory users through musl-nscd, or the `alpine` user in official tiny-cloud images
- At least one other active local account has a real password, stored as a `$5$` or `$6$` hash. sshd borrows its salt, so without it the attack fails. Check Point testing found the account must be active, not just hold a hash

What you can check remotely. Check Point testing found that two conditions show up before login. The SSH banner reveals the OpenSSH version. The server's list of allowed authentication methods shows whether it accepts passwords. A server that does not offer password authentication is not exposed. The rest (musl, PAM, account states, password hashes) needs a check on the host itself. Don't rely on the version string alone: Alpine's fixed packages keep older version numbers, such as 10.3_p1-r2 on Alpine 3.24, so a patched host can look vulnerable.

Root is safe under the default PermitRootLogin prohibit-password. But any reachable account with doas or sudo rights can still become root. glibc Linux, non-Linux systems, and Linux with PAM are not affected, per Damien Miller

of the OpenSSH team.

Fix and detect. Alpine ships patched packages for 3.16 through 3.24 and edge. Upgrade, then restart sshd, because the package upgrade does not restart the running daemon. Can't patch yet? Set PasswordAuthentication no. To check for compromise, search the logs for "Accepted password for" an account that has no password. If you can't rule out a login, treat the machine as compromised.

No CVE yet. No CVE is assigned as of November 5, 2026, so CVE-based scanners may not flag affected systems yet. Check musl-based hosts manually.

The OpenSSH team released the fix one day after learning of the bug. Its reason: AI agents now rediscover bugs, sometimes within hours, so long embargoes mainly help attackers.

Where OpenSSH Is Heading: Post-Quantum Crypto and Deprecations

Attackers can record encrypted traffic today and decrypt it once quantum computers mature. OpenSSH is moving to post-quantum cryptography to close that gap. It is also retiring legacy options, and some older clients and scripts will break.

The post-quantum path. ML-KEM hybrid key exchange (mlkem768x25519-sha256) arrives in 9.9 and becomes the default in 10.0. Since 10.1, the client warns when a connection uses non-post-quantum key exchange. In 10.6, the server logs the same warning. For signatures, an ML-DSA 44 + Ed25519 hybrid is experimental in 10.4 and fully enabled in 10.6. Regenerate any keys you made with the experimental version.

Change	Status	Who it affects
DSA keys	Removed in 10.0	Any system still using DSA host or user keys
Finite-field Diffie-Hellman in sshd	Off by default since 10.0	Old clients without elliptic-curve or post-quantum key exchange
Peers that cannot rekey	Fail since 10.3	Very old or non-conforming SSH implementations
ECC in libcrypto	Required since 10.5	Custom builds without elliptic-curve support
scp -R (remote-to-remote copy through the remote host)	Warns since 10.6; ignored in a future release	Scripts that use scp -R
SHA-1 SSHFP DNS records	Removal announced	DNS zones that publish only SHA-1 SSHFP records
Platforms that need root for PTYs and lack fd passing	Removal announced (QNX 6, SCO OpenServer 5)	Legacy embedded and Unix systems

Two more changes may need a config or monitoring review. The sshd split into sshd-session (9.8) and sshd-auth (10.0) changes process names in logs. In 10.1, agent sockets move from /tmp to ~/.ssh/agent.

What You Should Do Now

Upgrade to 10.6p2 or your distribution's patched build. Then work through the compatibility changes above.

1. **Patch exposed systems first.** Start with internet-facing sshd and musl-based Linux, such as Alpine containers, running sshd without PAM. Most distributions backport fixes, so check the vendor advisory, not just the version string. Restart sshd after upgrading. Can't patch yet? Set PasswordAuthentication no
2. **Retire legacy keys and algorithms.** Replace any DSA keys. Upgrade or retire clients that still need finite-field Diffie-Hellman
3. **Use the post-quantum warnings.** The WarnWeakCrypto server logs in 10.6 show you exactly which clients need an upgrade
4. **Turn off SSH compression** where trusted and untrusted traffic share a connection. Compress at the application level instead
5. **Fix scripts before the behavior changes.** Replace scp -R. Review any automation that builds ssh commands from outside input, like git URLs or inventory files
6. **Check agents and certificates.** Look for certificates with empty principal lists. Confirm your tooling finds agent sockets in ~/.ssh/agent
7. **Plan for more frequent updates.** Releases now land every one to two months. Track the release notes or the openssh-unix-announce mailing list

Sources

OpenSSH release notes, read November 5, 2026 (covers 9.8 through 10.6p2) · Alpine Linux security advisory: openssh-server password authentication bypass, November 5, 2026 · Damien Miller announcement of OpenSSH 10.6p2, November 5, 2026 · Red Hat Bugzilla 2553035: CVE-2026-110926 and OpenCVE entry · SentinelOne: CVE-2026-106555 · Crossing the Streams (Fabian Bäumer and Marcus Brinkmann, Ruhr University Bochum) · CyberInsider on regreSSHion and Gatewatcher on CVE-2024-6387