Download Security

Overview

cPanel & WHM versions 11.48 and later include functionality to validate that you download all cPanel & WHM-delivered files in an uncorrupted state. This avoids any possibility of corruption due to a compromise of the `next.cpanel.net` mirror system or the server's connection to cPanel, L.L.C. systems.

The signature verification logic requires that all assets you download from the `httpupdate` mirror system meet either of the following criteria:

- The system directly validates the assets through separate GnuPG (GPG) signature files.
- The assets are anchored to a signed asset with cryptographically-secure checksums.

The system validates assets that you download from other cPanel, L.L.C. systems, such as the public portion of our GPG keys, via SSL connections.

GPG Keys

cPanel & WHM uses two primary GPG keys to sign assets delivered through our `httpupdate` mirror system. The system uses release keys to sign all assets intended for the normal mirror system. The system uses development keys to sign internal development builds and builds destined for the `next.cpanel.net` mirror system.

cPanel & WHM systems that track release tiers or Long Term Support tiers only need access to the "release" keys. To track experimental development builds on the `next.cpanel.net` mirror system, you **must** enable the development keys.

Controls

The *Security* section of WHM's *Tweak Settings* interface (*WHM >> Home >> Server Configuration >> Tweak Settings*) contains the *Signature validation on assets downloaded from cPanel & WHM mirrors* setting. This setting controls the types of signatures that cPanel & WHM accepts and defaults to *Release Key Only.*

cPanel & WHM also provides support for custom third-party cPAddons Site Software installations. By default, cPanel & WHM **doesn't** validate the security of third-party cPAddons in the same way it does for cPanel & WHM-delivered cPAddons. If you know that all third-party cPAddons residing on the system system are correctly-signed, you can enable signature verification.

Failure Messages

If files that you download from the the `next.cpanel.net` mirror system mirrors become corrupt in transit, an error message that indicates what type of failure occurred will appear. Most cPanel & WHM subsystems will automatically switch to a different mirror to download a valid version of the requested file.

Error Message	Meaning
Requesting script ... Failed to download signature for URL ' http://httpupdate.cpanel.net/autofixer2/test' .	This failure message indicates that the `.asc` signature file which should accompany a download does not exist on the mirror.
Error: Failed to verify signature for cpanel (key types: release): Invalid signature.	This failure message indicates that a key in the correct keyring generated a signature file, but the file that the signature accompanies appears modified.
Error: Failed to verify signature for cpanel (key types: release): Could not find public key in keychain.	This message error indicates that a key does not exist in the currently-selected keyring's signature file. You may encounter this error message if you attempt to download a build from `next.cpanel.net` but do not enable the development keyring.

Checksum mismatch (actual: ce154dabbea49ff9ba30873964e8fd3736270ababaa35ffa574926818e9667f890fdbd3c3a04a54f5e12a009c0250b750cdcde1ed6888e4a8bac2749534ce56e) (expected: 3778908211e79f4c384ab707d6ce4f34b274bd997158fe9f33ffb2afd50f8e77920813134447245cfa54a47b945fadb639006fc4db3f9188137d00cf12ecefb0)	This message indicates that the checksum for an unsigned file did not match the expected value and you cannot use it safely.
Signature verification failed using file from IP 10.215.217.12 and signature from IP 10.215.217.24...skipping 10.215.217.12...	This message indicates that the following items did not validate correctly: • The file from the mirror at the `10.215.217.12` server. • The signature from the `10.215.217.24` server. In most cases, out-of-date mirrors rather than malicious tampering cause signature verification failures. cPanel & WHM's download logic attempts to download files and their matching signatures four times via different mirrors before it aborts the download.
Failed to create gpg object: No keys found for vendor 'cpanel'	This failure message indicates that a local copy of the cPanel GPG public key file (`cPanelPublicKey.asc`) does not exist on the server. The system downloads these keys from `https://securedownloads.cpanel.net/` during the nightly update process. You can manually download a cPanel GPG key update with the `/usr/local/cpanel/scripts/updatesigningkey` script.

Additional documentation

- Download Security
- Third-Party Software End Of Life Policy
- Upgrade Blockers
- cPanel Long-Term Support
- Interface Lock Scripts