F

FusionCore PUA: Bundled Software Detection and Removal

FusionCore is a Windows software bundler detected as a potentially unwanted application because it can install additional unwanted programs.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 Is FusionCore malware?
02 How bundled installation happens
03 Possible effects
04 How to remove FusionCore safely
05 How to prevent bundled software
06 Sources

Quick answer: FusionCore is a Windows software bundler classified by Microsoft as a potentially unwanted application (PUA). It is known to install additional potentially unwanted software and may affect the browsing or computing experience. Quarantine the detected installer or component, remove software it added, review browser and network

settings, and scan again.

01 Is FusionCore malware?

Security products commonly label FusionCore as PUA, adware, or a bundler rather than as one specific self-replicating virus. PUA classification describes software behavior and distribution that users may not expect or want. It does not mean every file with a similar name has identical behavior, nor should a detection be ignored because the label is not “Trojan.”

Microsoft says PUA:Win32/FusionCore has poor reputation, can affect the quality of the computing experience, and is known to install other unwanted applications. Malwarebytes describes its corresponding detection as a large family of Windows adware bundlers. The legitimate program advertised by an installer and the bundling component can receive different verdicts.

02 How bundled installation happens

A user downloads a free utility, media tool, converter, game-related program, or repackaged installer from a download portal or advertisement. The installer presents additional offers, sometimes through preselected choices, ambiguous buttons, or disclosures that are easy to miss. Accepting the default flow can install browser modifiers, advertising components, updaters, or other PUAs.

Names, offers, and file locations vary. A detection in a browser cache or Downloads folder may mean the file was downloaded but never executed, while detections in installed-program, startup, task, service, or browser-extension locations indicate more investigation is needed.

03 Possible effects

- Unexpected applications, browser extensions, shortcuts, or background updaters.
- Changed home page, search provider, new-tab behavior, proxy, or notification permissions.
- Advertisements, redirects, slower browsing, or unfamiliar processes.

- Repeated security alerts when a bundled component attempts to reinstall or update.

These symptoms are not unique to FusionCore. Use the security alert’s exact path, hash, parent process, and installation time to connect the detection to a particular download.

04 How to remove FusionCore safely

1. Do not run the detected installer again. Record the verdict and path, then allow the trusted security product to quarantine it.
2. Review recently installed applications by installation date. Uninstall items you did not knowingly choose, using the operating system’s normal uninstall process.
3. Remove unrecognized browser extensions and notification permissions. Verify the home page, search engine, startup pages, proxy, and DNS settings.
4. Update the security engine and run a full scan. If alerts return, use an offline scan and inspect scheduled tasks, services, startup entries, and other user profiles.
5. Reset passwords from a clean device only if evidence shows credential theft or a separate infostealer. FusionCore’s PUA label alone does not prove passwords were stolen.

If the file belongs to software you need, obtain a fresh installer directly from the official publisher. Do not create a broad antivirus exclusion for the Downloads folder or disable PUA protection simply to finish installation. Submit the exact file to the detecting vendor if you believe the classification is incorrect.

05 How to prevent bundled software

Download programs from the publisher or an official app store, verify the domain and digital signature, and reject optional offers. Avoid cracked or repackaged installers and deceptive download buttons. Keep browser reputation checks and potentially unwanted app blocking enabled. Organizations can use application allow-listing, managed app catalogs, web filtering, and standard-user accounts.

06 Sources

Classification and behavior are based on the Microsoft FusionCore description and Malwarebytes/ThreatDown detection reference.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com