PortfolioDAM

PORTFOLIO RELEASE NOTES

CURRENT VERSION 4.2

- Portfolio Server version 4.2 operates exclusively on Windows platforms.
- For deployments on macOS, please review our Apple Silicon and Rosetta 2 knowledge base article.
- Portfolio Media Engine: version 4.2
- Portfolio Web Client: version 4.2
- Portfolio Desktop Client: version 4.2

WHAT'S NEW IN PORTFOLIO 4.2

- **Server:** We updated Apache Tomcat to version 9.0.122. This resolved multiple security concerns, including information exposure (CVE-2021-43980, CVE-2023-42795), request smuggling issues (CVE-2023-45648, CVE-2023-46589, CVE-2026-24880), TLS handshake processing flaws when TLS terminates within Tomcat (CVE-2024-38286), security restriction circumvention (CVE-2026-24733), and open redirection vulnerabilities (CVE-2026-25854).
- **Server:** We updated Log4j from 2.17.2 to Reload 4j 1.2.26. This addressed an issue where Socket Appender fails to perform TLS hostname verification during connection establishment (CVE-2025-68161). Resolved a bug where appenders silently disregard the TLS verifyHostName configuration (CVE-2026-34477). Fixed XmlLayout generating invalid XML structure that led to lost log entries (CVE-2026-34480). Fixed malformed output generation within the Log4j 1 bridge XML layout (CVE-2026-34479). Resolved an issue where JSON Template Layout produces invalid JSON when handling floating-point numbers (CVE-2026-34481). Addressed invalid JSON generation by Log4j API when processing NaN and Infinity values (CVE-2026-49844).
- **Server:** We updated Java Runtime Environment from JRE 1.8.0_482 to Azul Zulu Java 8_502. This addressed a number of issues including: Resolved an unauthorized data access flaw within JAXP path factories (CVE-2026-22016). Addressed a zip file reading vulnerability affecting core libraries (CVE-2026-22018). Fixed a certificate chain validation weakness discovered in security libraries (CVE-2026-22021). Resolved a Kerberos credential handling security flaw within security components (CVE-2026-22013). Upgraded the bundled FreeType font library to patch a known vulnerability (CVE-2026-23865). Corrected a cryptographic algorithm support flaw causing potential local information exposure (CVE-2026-22007). Patched a key generation weakness that could lead to local information leakage (CVE-2026-34268). Updated the embedded LittleCMS color library to eliminate a denial-of-service vulnerability (CVE-2026-41254). Fixed a TLS certificate handling flaw present during secure connection establishment (CVE-2026-46968). Addressed a certification validation bug that compromised certificate trust decisions (CVE-2026-60147). Resolved a Jar archive processing weakness in security libraries (CVE-2026-47027). Patched an additional Jar processing vulnerability within security validation routines (CVE-2026-47063). Fixed a JPEG image processing vulnerability inside imaging components (CVE-2026-47010). Resolved an XBM image handling flaw within 2D graphics rendering (CVE-2026-47021). Corrected an AWT ImagingLib vulnerability identified in image manipulation code (CVE-2026-47059). Patched an index handling flaw in the Nashorn JavaScript engine (CVE-2026-47057). Addressed a DataView implementation weakness in the core JDK (CVE-2026-47058).
- **Server:** We updated Node.js from 8.9.2 to 8.9.4. This resolved a small number of issues including an OpenSSL error-state flaw enabling potential security bypass of TLS safeguards (CVE-2017-15896). Patched an internal OpenSSL SSL_read error handling bug that was resolved in version 1.0.2n (CVE-2017-3737).
- **Server:** We removed the requirement to run Portfolio Server on a Windows Server OS. Modern business workstations feature multi-core processors, expanded memory capacity from 16 to 64 GB RAM, alongside high-speed drives. Microsoft limits inbound connection requests on Windows 11 Pro to roughly 20 concurrent sessions. According to Microsoft support, Windows 11 Pro is suitable for small business environments as a micro server deployment supporting up to 3-5 clients. Windows desktop is NOT recommended for Portfolio Server Enterprise.
- **Server:** We updated the license server address to remove the Extensis license server and point to a new license server managed by PortfolioDAM LLC
- **Server:** We introduced new dynamic memory management to Portfolio Server to improve search performance and responsiveness.

- **Server:** We removed the optional check box in the Portfolio Server Admin console to send analytical information to Extensis.
- **Server:** We removed references and buttons to enable Smart Keywords which had been deprecated by Extensis.

WHAT CHANGED IN VERSION 4.0.1

- **Server:** Extensis updated Apache Tomcat to version 9.0.58.
- **Server:** Extensis updated the Log4j library to version 2.17.2. This resolved a security vulnerability identified in earlier versions of Log4j, details of which can be found in **CVE-2021-44228**.
- Server: Extensis addressed five other high-risk security flaws reported by **White Oak Security**:
- **Admin/Web/Desktop:** Resolved an authentication bypass flaw resulting from hard-coded credentials (CVE-2022-24255).
- **Web:** Patched an authenticated unrestricted file upload flaw leading to potential remote code execution (CVE-2022-24251).
- **Web:** Fixed an authenticated file upload and path traversal vulnerability causing remote code execution (CVE-2022-24252).
- **Admin:** Corrected an authenticated Zip-Slip archive path traversal flaw enabling remote code execution (CVE-2022-24254).
- **Admin:** Addressed an authenticated unrestricted file upload security weakness allowing remote code execution (CVE-2022-24253).

Please note: The security fix for CVE-2022-24252 may cause issues with custom Web Client scripts. If scripts fail to execute, please review our knowledge base article on script enablement.

WHAT CHANGED IN VERSION 4.0.0

- **Server:** Extensis Added compatibility support for Active Directory 2019 environments.
- Web, Desktop: Introduced functionality allowing users to share private galleries with team members.
- **Server:** Added an option to disable English language processing within the General Engine configuration under Smart Keywords preferences when selecting alternate languages.
- **Web, Desktop:** Enhanced NetPublish Site Builder to support publishing an unlimited number of metadata fields per catalog (verify field layout prior to publication).
- **NetPublish**: Expanded the display area for asset details within NetPublish preview windows.
- **NetPublish:** Added site builder configuration settings to grant visitors multi-format download options.
- **NetPublish**: Improved dynamic visual contrast for watermarks by applying white text shadows on dark overlays and black text shadows on light backgrounds.
- **NetPublish:** Introduced administrative policies governing visitor download behavior for un-watermarked asset types.
- **Server:** Extensis updated the LibRaw image library to version 0.20.2.
- **Server:** Extensis updated Apache Tomcat to version 9.0.43.
- **NetPublish:**Fixed a visual truncation issue affecting extended field names assigned to Grid Fields inside NetPublish Site Builder. [PORT-12930]
- **NetPublish:**Resolved a formatting bug causing corrupted account names within NetPublish Usage logs. [PORT-13127]
- **Server:** Corrected asset retention behavior where deleted files were removed prematurely from Asset Deletion reports regardless of configured date criteria. [PORT-13349]
- **Server:** Fixed metadata categorization errors placing EXIF and GEO properties into wrong groupings when creating catalogs in non-US English client sessions. [PORT-13354]
- **Server:** Fixed catalog creation failures occurring when applying the General Use template during International English language sessions. [PORT-13365]

© 2026 Portfolio DAM LLC · portfoliodam.com ·