AccurioPro Flux

ReadMe

for AccurioPro Flux Cumulative Security Patch 13.2026.1029

Document revision: 1

Last modified: 03.11.2026

This patch contains all security updates released for AccurioPro Flux so far.

It includes fixes for the following vulnerabilities:

FLX-9721 (October 2026/2)

A vulnerability in Node.js (CVE-2026-111497)

Affected editions: AccurioPro Flux Essential, Premium, Ultimate

Affected components: Flux Server, Flux Web

Patch can be applied to: 10.0.0 until 10.4.2.82678

Updated software: Disabled Brotli-Decoder in AccurioPro Flux v10.0 to v10.2.77844 to circumvent CVE-2026-111497 in those versions.

Possible RCE in the node-internal Brotli decoder. This patch disables that decoder on startup of Flux Web/Server leading to them being unaffected by the CVE.

To the best of our knowledge, these vulnerabilities have not been exploited in connection with AccurioPro Flux.

FLX-9721 (October 2026/1)

Several vulnerabilities in Node.js

Affected editions: AccurioPro Flux Essential, Premium, Ultimate

Affected components: Flux Server, Flux Web

Patch can be applied to: 10.2.2 until 10.4.2.82678

Updated to: Node.js 22.23.4, MongoDB 7.0.45

CVE-2026-105483, CVE-2026-111497, CVE-2026-106069, CVE-2026-105482

These CVEs affect hostname bypasses affecting TLS certificate verification; a DNS resolving issue and a possible RCE in the node-internal Brotli decoder.

To the best of our knowledge, these vulnerabilities have not been exploited.

FLX-9564 (October 2026)

Several vulnerabilities in MongoDB

Affected editions: AccurioPro Flux Essential, Premium, Ultimate

Affected components: Flux Server

Patch can be applied to: 10.0.0 until 10.4.2.82678

Updated to: Node.js 22.23.3, MongoDB 7.0.43

MongoDB is used as the main database for Flux Server.

The MongoDB instances used by Flux Server are not reachable over the network. An attacker would require access to the machine Flux Server is running on, therefore the risk posed by these vulnerabilities is low in the context of AccurioPro Flux. All vulnerabilities are considered not exploitable in the context of AccurioPro Flux.

To the best of our knowledge, these vulnerabilities have not been exploited.

FLX-9563 (October 2026)

7-Zip failed to preserve the Mark-of-the-Web when extracting a crafted archive. (CVE-2026-58052)

Affected editions: AccurioPro Flux Essential, Premium, Ultimate

Affected components: Flux Server

Patch can be applied to: 8.0 until 10.4.2.82678

7-Zip is used in the Backup/Restore feature of AccurioPro Flux for reading and writing backup files. The vulnerability in 7-Zip is not known to be actively exploited at the time of writing. We are not aware of any instance of AccurioPro Flux being targeted using this vulnerability.

FLX-9567 (October 2026)

A vulnerability in the Node.js path.join API where Windows drive letters are not treated as special, resulting in incorrect treatment of absolute paths as relative (CVE-2025-23084)

Affected editions: AccurioPro Flux Essential, Premium, Ultimate

Affected components: Flux Server, Flux Web, Flux Workstation

Patch can be applied to: 10.0.0 until 10.2.2.78563

Node.js is the central runtime component used by AccurioPro Flux.

To the best of our knowledge, this vulnerability has not been exploited.

FLX-9356 (August 2026)

Several vulnerabilities in MongoDB

Affected editions: AccurioPro Flux Essential, Premium, Ultimate

Affected components: Flux Server

Patch can be applied to: 10.0.0 until 10.4.2.82671

MongoDB is used as the main database for Flux Server.

The MongoDB instances used by Flux Server are not reachable over the network. An attacker would require access to the machine Flux Server is running on, therefore the risk posed by these vulnerabilities is low in the context of AccurioPro Flux. All vulnerabilities are considered not exploitable in the context of AccurioPro Flux.

To the best of our knowledge, these vulnerabilities have not been exploited.

FLX-9316 (August 2026)

Several vulnerabilities in MongoDB

Affected editions: AccurioPro Flux Essential, Premium, Ultimate

Affected components: Flux Server

Patch can be applied to: 10.0.0 until 10.4.2.82662

MongoDB is used as the main database for Flux Server. One of the vulnerabilities can potentially lead to a system crash in Flux Server.

The MongoDB instances used by Flux Server are not reachable over the network. An attacker would require access to the machine Flux Server is running on, therefore the risk posed by this vulnerability is low in the context of AccurioPro Flux.

To the best of our knowledge, these vulnerabilities have not been exploited.

FLX-9310 (August 2026)

Several vulnerabilities in Node.js (CVE-2026-56846, CVE-2026-56848)

Affected editions: AccurioPro Flux Essential, Premium, Ultimate

Affected components: Flux Server, Flux Web

Patch can be applied to: 10.0.0 until 10.4.2.82662

Node.js is the central runtime component used by AccurioPro Flux.

Some of the vulnerabilities can potentially lead to a denial-of-service attack in the Flux Web online shop.

To the best of our knowledge, these vulnerabilities have not been exploited.

Note that this update only applies to AccurioPro Flux versions 10.2.2 up to 10.4.2. To fix the vulnerabilities in environments running older versions of AccurioPro Flux, please update to the latest version. An active Software Maintenance Plan (SMP) is required.

FLX-9279 (July 2026)

A potential remote code execution vulnerability in 7-Zip (CVE-2026-14266)

Affected editions: AccurioPro Flux Essential, Premium, Ultimate

Affected components: Flux Server

Patch can be applied to: 8.0 until 10.4.2.82657

7-Zip is used in the Backup/Restore feature of AccurioPro Flux for reading and writing backup files. The vulnerability in 7-Zip is not known to be actively exploited at the time of writing. We are not aware of any instance of AccurioPro Flux being targeted using this vulnerability. It is strongly recommended for users to install this security patch.

FLX-9191 (June 2026)

Several vulnerabilities in Node.js

Affected editions: AccurioPro Flux Essential, Premium, Ultimate

Affected components: Flux Server, Flux Web

Patch can be applied to: 9.0 until 10.4.2.82645

Node.js is the central runtime component used by AccurioPro Flux.

Some of the vulnerabilities can potentially lead to a denial-of-service attack in the Flux Web online shop.

To the best of our knowledge, these vulnerabilities have not been exploited.

Note that this update only applies to AccurioPro Flux versions 10.2.2 up to 10.4.2. To fix the vulnerabilities in environments running older versions of AccurioPro Flux, please update to the latest version. An active Software Maintenance Plan (SMP) is required.

FLX-9185 (June 2026)

Several vulnerabilities in MongoDB

Affected editions: AccurioPro Flux Essential, Premium, Ultimate

Affected components: Flux Server

Patch can be applied to: 10.0 until 10.4.2.82645

MongoDB is used as the main database for Flux Server. The MongoDB instances used by Flux Server are not reachable over the network. All of the fixed vulnerabilities require the attacker to have access to the Flux Server machine. Additionally, all but one of the fixed vulnerabilities require the attacker to be an authenticated user in MongoDB. Therefore, the risk posed by these vulnerabilities is low in the context of AccurioPro Flux.

To the best of our knowledge, these vulnerabilities have not been exploited in connection with AccurioPro Flux.

FLX-9093 (June 2026)

A potential remote code execution vulnerability in 7-Zip (CVE-2026-48095)

Affected editions: AccurioPro Flux Essential, Premium, Ultimate

Affected components: Flux Server

Patch can be applied to: 8.0 until 10.4.2.82634

7-Zip is used in the Backup/Restore feature of AccurioPro Flux for reading and writing backup files. The vulnerability in 7-Zip is not known to be actively exploited at the time of writing. We are not aware of any instance of AccurioPro Flux being targeted using this vulnerability. It is strongly recommended for users to install this security patch.

FLX-8429 (January 2026)

A potential unauthorized memory read in MongoDB (Mongobleed, CVE-2025-14847)

Affected editions: AccurioPro Flux Essential, Premium, Ultimate

Affected components: Flux Server

Patch can be applied to: 7.0 until 10.2.2.78547

MongoDB is used as the main database for Flux Server. The MongoDB instances used by Flux Server are not reachable over the network. An attacker would require access to the machine

Flux Server is running on, therefore the risk posed by this vulnerability is low in the context of AccurioPro Flux.

To the best of our knowledge, this vulnerability has not been exploited in connection with AccurioPro Flux.

Note that this update only applies to Flux versions 10.0.0 through 10.2.2.To fix the vulnerabilities in environments running older versions of AccurioPro Flux, please update to the latest version. An active Software Maintenance Plan (SMP) is required.

FLX-8525 (January 2026)

A potential denial-of-service vulnerability in Node.js HTTP/2 (CVE-2025-59465)

Affected editions: AccurioPro Flux Ultimate

Affected components: Flux Web

Patch can be applied to: 9.0 until 10.2.2.78547

This vulnerability can potentially lead to a denial-of-service in the Flux Web online shop.

To the best of our knowledge, this vulnerability has not been exploited.

Note that this update only applies to Flux version 10.2.2. To fix the vulnerabilities in environments running older versions of AccurioPro Flux, please update to the latest version. An active Software Maintenance Plan (SMP) is required.

FLX-8261 (November 2025)

A potential remote code execution vulnerability in 7-Zip (CVE-2025-11001)

Affected editions: AccurioPro Flux Essential, Premium, Ultimate

Affected components: Flux Server

Patch can be applied to: 8.0 until 10.2.2.78546

7-Zip is used in the Backup/Restore feature of AccurioPro Flux for reading and writing backup files. The vulnerability in 7-Zip is known to be actively exploited, although we are not aware of any instance of AccurioPro Flux being targeted. It is strongly recommended for users to install this security patch or update to the latest version.

FLX-8118 (November 2025)

A potential remote code execution vulnerability in ImageMagick (CVE-2025-57807)

Affected editions: AccurioPro Flux Essential, Premium, Ultimate

Affected components: Flux Server, Flux Web, Flux Workstation

Patch can be applied to: 8.0 until 10.2.2.78536

To the best of our knowledge, this vulnerability has not been actively exploited.

FLX-7425 (May 2025)

A remote code execution vulnerability in a third-party component used by AccurioPro Flux which can allow attackers to execute malicious code on the system running AccurioPro Flux.

Affected editions: AccurioPro Flux Essential, Premium, Ultimate

Affected components: Flux Server, Flux Web

Patch can be applied to: 8.4.0 until 10.2.0.77842

This issue was discovered through internal penetration testing and, to the best of our knowledge, is not being actively exploited or known publicly.

FLX-7411 (May 2025)

A denial-of-service vulnerability in AccurioPro Flux Web that can be used to cause a service outage by causing the Flux Web server to crash.

Affected editions: AccurioPro Flux Essential, Premium, Ultimate

Affected components: Flux Web

Patch can be applied to: 10.0.0 until 10.2.0.77842

This issue was discovered internally and, to the best of our knowledge, is not being actively exploited or known publicly.

FLX-6554 (September 2024)

The remote code execution vulnerability known as 'ImageTragick' (CVE-2016–3714)

This vulnerability was previously fixed in a separate patch installer in September 2024. It could allow the unauthorized execution of external code.

Affected editions: AccurioPro Flux Essential, Premium, Ultimate

Affected components: Flux Server, Flux Web, Flux Workstation

Patch can be applied to: 8.0 until 10.2.0.77842

To the best of our knowledge, this vulnerability has not been actively exploited.

Installation

The patch applies to all versions of AccurioPro Flux from 8.0.0 through 10.4.2.82678. It will automatically fix the vulnerabilities contained in the respective version.

It needs to be installed on every machine where one or more affected components of AccurioPro Flux are installed (e.g. Flux Server, Flux Web or Flux Workstation).

To install the patch, simply run the provided EXE file and follow the on-screen instructions.

Notes

- If the patch installer is used on the Flux Server PC, the Flux Server service will automatically be stopped during installation of the patch and restarted afterwards.
- If the patch installer is used on the Flux Web PC, the Flux Web service will automatically be stopped during installation of the patch and restarted afterwards.
- If Flux Workstation is installed at a later date via the installer on the Flux Server download page, the patch installer must be run afterwards.
- The installer can be run again after it has been updated with patches for new vulnerabilities.

All information for this documentation has been compiled with care, but is provided without warranty of any kind.

No portion of this documentation or the program may be reproduced or distributed on electronic or other media in any form (print, photocopy, microfilm or other method) without the prior written permission of dots Gesellschaft für Softwareentwicklung mbH.

AccurioPro is a trademark of Konica Minolta, Inc. All other brand names and product names belong to the respective companies and are protected by international trademark, brand and patent laws.

All rights reserved.

dots Gesellschaft für Softwareentwicklung mbH
Schlesische Straße 27 | 10997 Berlin | Germany
info@dots-software.com | www.dots-software.com

Konica Minolta Business Solutions Europe GmbH
Europaallee 17 | 30855 Langenhagen | Germany
Phone +49 (0) 511 74040 | www.konicaminolta.eu