



# CVE-2023-27873

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2023-27873
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@us.ibm.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-03-21 15:15:00 UTC
<b>Updated</b>	2023-11-07 04:10:00 UTC
<b>Description</b>	IBM Aspera Faspex 4.4.2 could allow a remote authenticated attacker to obtain sensitive credential information using speci

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">ibm</a>	<a href="#">Aspera Faspex</a>	4.4.2	patch_level_1	All	All
Application	<a href="#">ibm</a>	<a href="#">Aspera Faspex</a>	4.4.2	patch_level_2	All	All
Application	<a href="#">ibm</a>	<a href="#">Aspera Faspex</a>	All	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	-	All	All	All

## References

### Reference

Security Bulletin: IBM Aspera Faspex 4.4.2 PL3 has addressed multiple vulnerabilities (CVE-2023-27871, CVE-2023-27873, CVE-2023-27874)

[IBM X-Force Exchange](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[730775 IBM Aspera Faspex Multiple Security Vulnerabilities \(6964694\)](#)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)