ADV2026_196 IBM Security Advisory (March 31st, 2026)

IBM published a security advisory highlighting vulnerabilities in the following product between March 23 and 29, 2026. It is recommended that you take the necessary precautions by ensuring your products are always updated.

- Communications Server for AIX – version 6.4
- Communications Server for Data Center Deployment – versions 7.0 to 7.1
- Communications Server for Linux on System z – version 6.4
- Communications Server for Linux – version 6.4
- DataPower Operations Dashboard – versions 1.0.23.1 to 1.0.23.2
- DataStage on Cloud Pak for Data – version 5.3.1
- IBM App Connect Enterprise Certified Containers Operands – multiple versions
- IBM App Connect Enterprise – versions 12.0.1.0 to 12.0.12.23
- IBM App Connect Enterprise – versions 13.0.1.0 to 13.0.6.2
- IBM App Connect Operator – multiple versions
- IBM CICS TX Standard – version 11.1
- IBM Common Licensing – multiple versions
- IBM DevOps Release – versions 7.0.0 to 7.0.0.5
- IBM Event Endpoint Management – versions 11.0.0 to 11.7.2
- IBM Industry Solutions Workbench – version 5.0.0.0 and 5.1.0.0
- IBM InfoSphere Optim Archive Viewer – versions 11.7 FixPack09 to 11.7 FixPack12
- IBM Knowledge Catalog Standard Cartridge – multiple versions
- IBM MQ Operator – multiple versions
- IBM Security QRadar Log Management AQL Plugin – versions 1.0.0 to 1.1.3
- IBM SPSS Modeler – multiple versions
- IBM Storage Protect Operations Center – version 8.2.0
- IBM WebSphere Automation – versions 1.11.0 to 1.11.1
- IBM supplied MQ Advanced container images – multiple versions
- IBM watsonx Code Assistant On Prem – multiple versions
- IBM webMethods BPM – version 11.1 and 10.15

- InfoSphere Information Server – versions 11.7.0.0 to 11.7.1.6
- SOAR App Host – multiple versions
- Sterling Connect:Direct FTP+ – versions 1.3.0.0 to 1.3.0.3
- UCB - IBM UrbanCode Build – version 6.1.7 to 6.1.7.9
- UCR - IBM UrbanCode Release – versions 6.2.5 to 6.2.5.11
- WebSphere Extreme Scale – version 8.6.1.0 to 8.6.1

For more information on these updates, you can follow this URL:

- IBM Product Security Incident Response

The Guyana National CIRT recommends that users and administrators review these updates and apply them where necessary.

References

- IBM Product Security Incident Response. (n.b.). Retrieved from IBM. https://www.ibm.com/support/pages/bulletin/

- IBM security advisory. (March 30, 2026). Retrieved from Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/alerts-advisories/ibm-security-advisory-av26-294