

TIBCO Security Advisory: March 08, 2012 - TIBCO ActiveMatrix BusinessWorks™

Frequently Asked Questions

General FAQ

Why is this advisory being issued?

Security vulnerabilities have been discovered in:

- TIBCO ActiveMatrix® BPM below 1.3.0
- TIBCO ActiveMatrix BusinessWorks™ below 5.9.3
- TIBCO ActiveMatrix BusinessWorks™ Service Engine below 5.8.2
- TIBCO ActiveMatrix BusinessWorks Service Engine version 5.9.X below 5.9.3
- TIBCO ActiveMatrix BusinessWorks™ Distribution for TIBCO Silver® Fabric 5.9.2
- TIBCO ActiveMatrix® Service Bus version 2.X below 2.3.2
- TIBCO ActiveMatrix Service Bus version 3.X below 3.1.5
- TIBCO ActiveMatrix® Service Grid version 2.X below 2.3.2
- TIBCO ActiveMatrix Service Grid version 3.X below 3.1.5
- TIBCO ActiveMatrix® Service Grid Distribution for TIBCO Silver® Fabric 3.1.3
- TIBCO BusinessEvents® Enterprise Edition version 3.X below 3.0.3
- TIBCO BusinessEvents® Inference Edition version 3.X below 3.0.3
- TIBCO BusinessEvents® Standard Edition version 4.X below 4.0.2
- TIBCO BusinessEvents® Standard Edition version 5.0.0
- TIBCO BusinessEvents® Express version 5.0.0
- TIBCO Spotfire® Analytics Server below 10.1.2
- TIBCO Spotfire® Server below 3.1.3
- TIBCO Spotfire Server 3.2.X versions below 3.2.2
- TIBCO Spotfire Server 3.3.X versions below 3.3.3
- TIBCO Spotfire® Web Player below 3.1.1
- TIBCO Spotfire Web Player 3.2.X versions below 3.2.2
- TIBCO Spotfire Web Player 3.3.X versions below 3.3.2
- TIBCO Spotfire Web Player 4.0.X versions below 4.0.2
- TIBCO Spotfire® Automation Services below 3.1.1
- TIBCO Spotfire Automation Services 3.2.X versions below 3.2.2
- TIBCO Spotfire Automation Services 3.3.X versions below 3.3.2
- TIBCO Spotfire Automation Services 4.0.X versions below 4.0.2
- TIBCO Spotfire® Professional below 3.1.1
- TIBCO Spotfire Professional 3.2.x versions below 3.2.2
- TIBCO Spotfire Professional 3.3.x versions below 3.3.2
- TIBCO Spotfire Professional 4.0.x versions below 4.0.2

What is the impact of these vulnerabilities?

The impact of these vulnerabilities may include information modification, information disclosure, and denial of service. For details, please see the [security advisory](#).

Which customers are affected?

These issues affect all customers using the above product versions.

Where can I get software updates?

Customers with current maintenance for the affected products can obtain product updates through their standard TIBCO fulfillment channel.

How will customers who receive TIBCO software via OEM partners be affected?

Customers of OEM partners can receive new versions and hot fixes from their OEM partners. Please contact your OEM partner for updates.

Can I get the software update if I am not current on maintenance, if I do not have access to the download site or access to TIBCO Support?

Please [contact TIBCO Support by telephone](#). Please reference SR:1-CTZA3R in your communication to indicate the context of your request.

What is TIBCO doing to prevent future security issues?

TIBCO takes security very seriously. We perform rigorous testing for every product release, as well as code audits, structured walkthroughs and peer reviews. TIBCO has identified security vulnerabilities in products during internal testing and reviews and corrected them prior to release. TIBCO constantly evaluates and augments its security measures and will continue to do so.

Where can I get more information?

Product advisories can be accessed from the [Security Advisories for TIBCO Products](#) web page.

Customers with a current maintenance contract with TIBCO can log a service request with TIBCO Global Support (please refer to the service request identifier listed above) and then call your support telephone number. Maintenance customers can also view product-specific Late Breaking News through the [TIBCO Support Web](#).

TIBCO ActiveMatrix BPM

Which product versions are affected?

- TIBCO ActiveMatrix BPM below 1.3.0

What components are affected?

- TIBCO ActiveMatrix Platform

How should customers handle these issues?

For each affected system, customers should update to:

- TIBCO ActiveMatrix BPM version 1.3.0 or higher

Please follow the instructions in the product installation manual.

What is updated by this new product version?

Please see the readme, release notes and/or documentation for a complete list of changes.

TIBCO ActiveMatrix BusinessWorks

Which product versions are affected?

- TIBCO ActiveMatrix BusinessWorks below 5.9.3

What components are affected?

- TIBCO BusinessWorks Engine

How should customers handle these issues?

For each affected system, customers should update to:

- TIBCO ActiveMatrix BusinessWorks 5.9.3 or higher

Please follow the instructions in the product installation manual. Note that TIBCO ActiveMatrix BusinessWorks 5.9.3 requires the following companion upgrades:

- TIBCO Runtime Agent™ 5.7.3
- TIBCO Administrator™ 5.7.1

What is updated by this new product version?

Please see the readme, release notes and/or documentation for a complete list of changes.

What other TIBCO products include TIBCO ActiveMatrix BusinessWorks?

- TIBCO® ActiveFullfillment

TIBCO ActiveMatrix BusinessWorks Service Engine

Which product versions are affected?

- TIBCO ActiveMatrix BusinessWorks Service Engine below 5.8.2
- TIBCO ActiveMatrix BusinessWorks Service Engine version 5.9.X below 5.9.3

What components are affected?

- TIBCO ActiveMatrix Platform

How should customers handle these issues?

For each affected system, customers should update to:

- TIBCO ActiveMatrix BusinessWorks Service Engine 5.8.X version 5.8.2 or higher
- TIBCO ActiveMatrix BusinessWorks Service Engine 5.9.3 or higher

Please follow the instructions in the product installation manual.

What is updated by this new product version?

Please see the readme, release notes and/or documentation for a complete list of changes.

TIBCO ActiveMatrix BusinessWorks Distribution for TIBCO Silver Fabric

Which product versions are affected?

- TIBCO ActiveMatrix BusinessWorks Distribution for TIBCO Silver Fabric 5.9.2

What components are affected?

- TIBCO BusinessWorks Engine

How should customers handle these issues?

For each affected system, customers should update to:

- TIBCO ActiveMatrix BusinessWorks Distribution for TIBCO Silver Fabric 5.9.3 or higher

Please follow the instructions in the product installation manual.

What is updated by this new product version?

Please see the readme, release notes and/or documentation for a complete list of changes.

TIBCO ActiveMatrix Service Bus

Which product versions are affected?

- TIBCO ActiveMatrix Service Bus version 2.X below 2.3.2

- TIBCO ActiveMatrix Service Bus version 3.X below 3.1.5

What components are affected?

- TIBCO ActiveMatrix Platform

How should customers handle these issues?

For each affected system, customers should update to:

- TIBCO ActiveMatrix Service Bus 2.X version 2.3.2 or higher
- TIBCO ActiveMatrix Service Bus 3.1.5 or higher

Please follow the instructions in the product installation manual.

What is updated by this new product version?

Please see the readme, release notes and/or documentation for a complete list of changes.

TIBCO ActiveMatrix Service Grid

Which product versions are affected?

- TIBCO ActiveMatrix Service Grid version 2.X below 2.3.2
- TIBCO ActiveMatrix Service Grid version 3.X below 3.1.5

What components are affected?

- TIBCO ActiveMatrix Platform

How should customers handle these issues?

For each affected system, customers should update to:

- TIBCO ActiveMatrix Service Grid 2.X version 2.3.2 or higher
- TIBCO ActiveMatrix Service Grid 3.1.5 or higher

Please follow the instructions in the product installation manual.

What is updated by this new product version?

Please see the readme, release notes and/or documentation for a complete list of changes.

TIBCO ActiveMatrix Service Grid Distribution for TIBCO Silver Fabric

Which product versions are affected?

- TIBCO ActiveMatrix Service Grid Distribution for TIBCO Silver Fabric 3.1.3

What components are affected?

- TIBCO ActiveMatrix Platform

How should customers handle these issues?

For each affected system, customers should update to:

- TIBCO ActiveMatrix Service Grid Distribution for TIBCO Silver Fabric 3.1.5 or higher

Please follow the instructions in the product installation manual.

What is updated by this new product version?

Please see the readme, release notes and/or documentation for a complete list of changes.

TIBCO BusinessEvents

Which product versions are affected?

- TIBCO BusinessEvents Enterprise Edition version 3.X below 3.0.3
- TIBCO BusinessEvents Inference Edition version 3.X below 3.0.3
- TIBCO BusinessEvents Standard Edition version 4.X below 4.0.2
- TIBCO BusinessEvents Standard Edition version 5.0.0
- TIBCO BusinessEvents Express version 5.0.0

What components are affected?

- TIBCO BusinessEvents Runtime

How should customers handle these issues?

For each affected system, customers should update to:

- TIBCO BusinessEvents Enterprise Edition 3.X version 3.0.3 or higher
- TIBCO BusinessEvents Inference Edition 3.X version 3.0.3 or higher
- TIBCO BusinessEvents Standard Edition 4.X version 4.0.2 or higher
- TIBCO BusinessEvents Standard Edition version 5.0.1 or higher
- TIBCO BusinessEvents Express version 5.0.1 or higher

Please follow the instructions in the product installation manual.

What is updated by this new product version?

Please see the readme, release notes and/or documentation for a complete list of changes. Note that TIBCO BusinessEvents 3.0.3 requires the following companion upgrades:

- TIBCO Runtime Agent™ 5.7.3
- TIBCO Administrator™ 5.7.1

What other TIBCO products include TIBCO BusinessEvents?

- TIBCO® ActiveFullfillment

TIBCO Spotfire Analytics Server

Which product versions are affected?

- TIBCO Spotfire Analytics Server below 10.1.2

What components are affected?

- TIBCO Spotfire Web Application

How should customers handle these issues?

For each affected system, customers should update to:

- TIBCO Spotfire Analytics Server version 10.1.2 or higher

Please follow the instructions in the product installation manual.

What is updated by this new product version?

Please see the readme, release notes and/or documentation for a complete list of changes.

TIBCO Spotfire Server

Which product versions are affected?

- TIBCO Spotfire Server below 3.1.3
- TIBCO Spotfire Server 3.2.X versions below 3.2.2
- TIBCO Spotfire Server 3.3.X versions below 3.3.3

What components are affected?

- TIBCO Spotfire Web Application

How should customers handle these issues?

For each affected system, customers should update to:

- TIBCO Spotfire Server 3.1.X version 3.1.3 or higher
- TIBCO Spotfire Server 3.2.X version 3.2.2 or higher
- TIBCO Spotfire Server 3.3.3 or higher

Please follow the instructions in the product installation manual.

What is updated by this new product version?

Please see the readme, release notes and/or documentation for a complete list of changes.

What other TIBCO products include TIBCO Spotfire Server?

- TIBCO DataSynapse™ Analytics

TIBCO Spotfire Web Player

Which product versions are affected?

- TIBCO Spotfire Web Player below 3.1.1
- TIBCO Spotfire Web Player 3.2.X versions below 3.2.2
- TIBCO Spotfire Web Player 3.3.X versions below 3.3.2
- TIBCO Spotfire Web Player 4.0.X versions below 4.0.2

What components are affected?

- TIBCO Spotfire Web Player Application

How should customers handle these issues?

For each affected system, customers should update to:

- TIBCO Spotfire Web Player 3.1.X version 3.1.1 or higher
- TIBCO Spotfire Web Player 3.2.X version 3.2.2 or higher
- TIBCO Spotfire Web Player 3.3.X version 3.3.2 or higher
- TIBCO Spotfire Web Player 4.0.2 or higher

Please follow the instructions in the product installation manual.

What is updated by this new product version?

Please see the readme, release notes and/or documentation for a complete list of changes.

What other TIBCO products include TIBCO Spotfire Web Player?

- TIBCO DataSynapse Analytics

TIBCO Spotfire Automation Services

Which product versions are affected?

- TIBCO Spotfire Automation Services below 3.1.1
- TIBCO Spotfire Automation Services 3.2.X versions below 3.2.2
- TIBCO Spotfire Automation Services 3.3.X versions below 3.3.2
- TIBCO Spotfire Automation Services 4.0.X versions below 4.0.2

What components are affected?

- TIBCO Spotfire Automation Services Application

How should customers handle these issues?

For each affected system, customers should update to:

- TIBCO Spotfire Automation Services 3.1.X version 3.1.1 or higher
- TIBCO Spotfire Automation Services 3.2.X version 3.2.2 or higher
- TIBCO Spotfire Automation Services 3.3.X version 3.3.2 or higher
- TIBCO Spotfire Automation Services 4.0.2 or higher

Please follow the instructions in the product installation manual.

What is updated by this new product version?

Please see the readme, release notes and/or documentation for a complete list of changes.

TIBCO Spotfire Professional

Which product versions are affected?

- TIBCO Spotfire Professional below 3.1.1
- TIBCO Spotfire Professional 3.2.x versions below 3.2.2
- TIBCO Spotfire Professional 3.3.x versions below 3.3.2
- TIBCO Spotfire Professional 4.0.x versions below 4.0.2

What components are affected?

- TIBCO Spotfire Analytics Client Application

How should customers handle these issues?

For each affected system, customers should update to:

- TIBCO Spotfire Professional 3.1.X version 3.1.1 or higher
- TIBCO Spotfire Professional 3.2.X version 3.2.2 or higher
- TIBCO Spotfire Professional 3.3.X version 3.3.2 or higher
- TIBCO Spotfire Professional 4.0.2 or higher

Please follow the instructions in the product installation manual.

What is updated by this new product version?

Please see the readme, release notes and/or documentation for a complete list of changes.

What other TIBCO products include TIBCO Spotfire Professional?

- TIBCO DataSynapse Analytics