

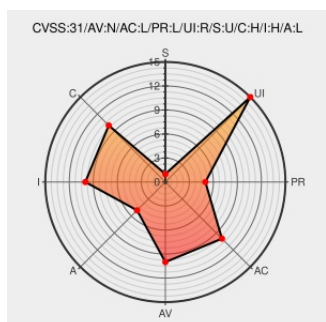


# CVE-2021-28828

Published on: 04/20/2021 12:00:00 AM UTC

Last Modified on: 04/23/2021 09:20:00 PM UTC

## CVE-2021-28828

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Administrator](#) from [Tibco](#) contain the following vulnerability:

The Administration GUI component of TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise

Edition for z/Linux, and TIBCO Administrator - Enterprise Edition for z/Linux contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute a SQL injection attack on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.10.2 and below, and TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.11.0 and 5.11.1.

CVE-2021-28828 has been assigned by [security@tibco.com](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>LOW</b>          | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **6.5 - MEDIUM**

| Access Vector  | Access Complexity | Authentication |
|----------------|-------------------|----------------|
| <b>NETWORK</b> | <b>LOW</b>        | <b>SINGLE</b>  |

| Confidentiality Impact | Integrity Impact | Availability Impact |
|------------------------|------------------|---------------------|
| PARTIAL                | PARTIAL          | PARTIAL             |

## CVE References

| Description                                                                                                      | Tags                                                       | Link                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Advisory   TIBCO Software                                                                                        | <a href="#">www.tibco.com</a><br><a href="#">text/html</a> |  CONFIRM <a href="https://www.tibco.com/services/support/advisories">www.tibco.com/services/support/advisories</a>                                                                                                                                         |
| TIBCO Security Advisory: April 20, 2021 - TIBCO Administrator - Enterprise Edition - 2021-28828   TIBCO Software | <a href="#">www.tibco.com</a><br><a href="#">text/html</a> |  CONFIRM <a href="https://www.tibco.com/support/advisories/2021/04/tibco-security-advisory-april-20-2021-tibco-administrator-2021-28828">www.tibco.com/support/advisories/2021/04/tibco-security-advisory-april-20-2021-tibco-administrator-2021-28828</a> |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

| Type        | Vendor                | Product                       | Version | Update | Edition | Language |
|-------------|-----------------------|-------------------------------|---------|--------|---------|----------|
| Application | <a href="#">Tibco</a> | <a href="#">Administrator</a> | 5.11.0  | All    | All     | All      |
| Application | <a href="#">Tibco</a> | <a href="#">Administrator</a> | 5.11.0  | All    | All     | All      |
| Application | <a href="#">Tibco</a> | <a href="#">Administrator</a> | 5.11.0  | All    | All     | All      |
| Application | <a href="#">Tibco</a> | <a href="#">Administrator</a> | 5.11.1  | All    | All     | All      |
| Application | <a href="#">Tibco</a> | <a href="#">Administrator</a> | 5.11.1  | All    | All     | All      |
| Application | <a href="#">Tibco</a> | <a href="#">Administrator</a> | 5.11.1  | All    | All     | All      |
| Application | <a href="#">Tibco</a> | <a href="#">Administrator</a> | All     | All    | All     | All      |
| Application | <a href="#">Tibco</a> | <a href="#">Administrator</a> | All     | All    | All     | All      |
| Application | <a href="#">Tibco</a> | <a href="#">Administrator</a> | All     | All    | All     | All      |

```
cpe:2.3:a:tibco:administrator:5.11.0:*:*:*:enterprise:*:*:*:
```

```
cpe:2.3:a:tibco:administrator:5.11.0:*:*:*:enterprise:silver_fabric:*:*:
```

```
cpe:2.3:a:tibco:administrator:5.11.0:*:*:enterprise:z\linux:*:*:
```

```
cpe:2.3:a:tibco:administrator:5.11.1:*:*:*:enterprise:*:*:*
```

```
cpe:2.3:a:tibco:administrator:5.11.1:*:*:*:enterprise:silver_fabric:*:*:
```

```
cpe:2.3:a:tibco:administrator:5.11.1.*:*:*:enterprise:z\linux:*:*:
```

```
cpe:2.3:a:tibco:administrator:*:*:*:enterprise:*:*:
```

```
cpe:2.3:a:tibco:administrator:*:*:*:enterprise:silver_fabric:*:*:
```

cpe:2.3:a:tibco:administrator:\*:\*:\*:\*:enterprise:z/linux:\*:\*:

No vendor comments have been submitted for this CVE

#### Social Mentions

| Source                        | Title | Posted (UTC)             |
|-------------------------------|-------|--------------------------|
| <a href="#">← Previous ID</a> |       | <a href="#">Next ID→</a> |

© [CVE.report](#) 2023   |

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](#).

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