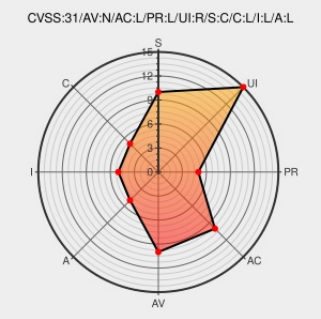
CVE-2021-28829

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

Last Modified on: 04/23/2021 09:19:00 PM UTC

CVE-2021-28829

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 persistent CSV injection attack from the affected system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. 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-2021-28829 has been assigned by security@tibco.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6 - MEDIUM

Access Vector	Access Complexity	Authentication

NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Advisory | TIBCO Software	www.tibco.com text/html	CONFIRM www.tibco.com/services/support/advisories
TIBCO Security Advisory: April 20, 2021 - TIBCO Administrator - Enterprise Edition - 2021-28829 | TIBCO Software	www.tibco.com text/html	CONFIRM www.tibco.com/support/advisories/2021/04/tibco-security-advisory-april-20-2021-tibco-administrator-2021-28829

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tibco	Administrator	5.11.0	All	All	All
Application	Tibco	Administrator	5.11.0	All	All	All
Application	Tibco	Administrator	5.11.0	All	All	All
Application	Tibco	Administrator	5.11.1	All	All	All
Application	Tibco	Administrator	5.11.1	All	All	All
Application	Tibco	Administrator	5.11.1	All	All	All
Application	Tibco	Administrator	All	All	All	All
Application	Tibco	Administrator	All	All	All	All
Application	Tibco	Administrator	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)

← Previous ID

Next ID→