مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Tableau Server

Tracking #:432317632

Date:25-08-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Tableau Server that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Vulnerability Details

- CVE-2025-26496 (CVSS 9.6 – Critical):
  A Type Confusion vulnerability in the File Upload modules of Tableau Server and Tableau Desktop could lead to Local Code Inclusion.
- CVE-2025-26497 and CVE-2025-26498 (CVSS 7.7 – High):
  Dangerous File Upload vulnerabilities in the Flow Editor and establish-connection-no-undo modules allowed Absolute Path Traversal.
- CVE-2025-52450 (CVSS 8.5 – High):
  An Improper Limitation of Pathname in the tabdoc API could enable Path Traversal and unauthorized file access.
- CVE-2025-52451 (CVSS 8.5 – High):
  An Improper Input Validation issue in the tabdoc API allowed Absolute Path Traversal.

Impact: Exploitation of these vulnerabilities could allow attackers to execute arbitrary code, bypass directory protections, gain unauthorized access to files, and manipulate file uploads.

Affected Versions

- Tableau Server before 2025.1.3
- Tableau Server before 2024.2.12
- Tableau Server before 2023.3.19

Fixed Versions

- 2025.1.4 or later
- 2024.2.13 or later
- 2023.3.20 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed version released by the Tableau Server.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://help.salesforce.com/s/articleView?id=005132575&type=1