مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerabilities in Tableau Server

Tracking #:432317544

Date:28-07-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Salesforce has released a security advisory addressing eight serious vulnerabilities affecting multiple versions of Tableau Server, the widely used data visualization and business intelligence platform.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **Unauthorized Database Access via Arbitrary SQL**
  (CVE-2025-52446, CVE-2025-52447, CVE-2025-52448)
  These vulnerabilities arise from improper authorization controls within Tableau's tab-doc API, specifically the set-initial-sql and validate-initial-sql features. Exploiting these flaws allows attackers to manipulate session-level settings and execute arbitrary SQL statements on production database clusters, potentially leading to unauthorized data access, modification, or exfiltration.
- **Remote Code Execution via Malicious File Upload**
  (CVE-2025-52449)
  A critical vulnerability in Tableau's Extensible Protocol Service allows unrestricted file uploads. Attackers can disguise malicious executables with deceptive filenames, upload them to the server, and trigger remote code execution, fully compromising the affected system.
- **Absolute Path Traversal Leading to Sensitive File Exposure**
  (CVE-2025-52452)
  This flaw in the duplicate-data-source module of the tabdoc API allows attackers to bypass directory restrictions and read arbitrary files on the host system. This could expose sensitive configuration files, credentials, and internal logs.
- **Server-Side Request Forgery (SSRF) in Multiple Components**
  (CVE-2025-52453, CVE-2025-52454, CVE-2025-52455)
  SSRF vulnerabilities exist in the Flow Data Source, Amazon S3 Connector, and EPS Server modules. These allow attackers to craft requests that make Tableau Server initiate unauthorized network connections to internal or external systems, potentially targeting cloud metadata services, internal administrative interfaces, or restricted databases.

Exploitation of these vulnerabilities could lead to:

- Unauthorized access to production databases
- Full remote code execution on Tableau Server
- Exposure of sensitive files and credentials
- Unauthorized internal or external network access via SSRF

Affected Versions

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

RECOMMENDATIONS:

- Apply the latest security patches immediately to affected Tableau Server versions

- Review server and network logs for any suspicious activity related to these vulnerabilities
- Restrict file upload permissions and monitor network traffic for anomalous connections

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=005105043&type=1