مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Notice No.	**:**	**CBUAE/BIS/2025/4158**
Date	**:**	**28/07/2025**
Classification	**:**	**Restricted**
To	**:**	**All Licensed Financial Institutions**
Attention	**:**	**Chief Executive Officer / Managing Director / General Manager**
Subject	**:**	**Cyber Security Advisory**

After greetings,

The UAE Cyber Security Council has observed the following vulnerabilities and security updates:

1) **Multiple critical vulnerabilities in the Tridium Niagara Framework that could be exploited for remote code execution, compromise of credentials, and persistent backdoor access, potentially leading to full system takeover.** Refer to the enclosed copy of the UAE Cyber Security Council Advisory, 'Ref: 432317543, Multiple Critical Vulnerabilities in Tridium Niagara Framework', dated 28 July 2025, with specific recommendations against increased cyber threats;

2) **Salesforce has released a security advisory addressing eight serious vulnerabilities affecting multiple versions of Tableau Server.** Refer to the enclosed copy of the UAE Cyber Security Council Advisory, 'Ref: 432317544, High-Severity Vulnerabilities in Tableau Server', dated 28 July 2025, with specific recommendations against increased cyber threats; and

3) **Critical vulnerability in Node-SAML that could potentially be exploited to bypass authentication controls in affected systems.** Refer to the enclosed copy of the UAE Cyber Security Council Advisory, 'Ref: 432317546, Critical Authentication Bypass Vulnerability in Node-SAML', dated 28 July 2025, with specific recommendations against increased cyber threats.

The Central Bank of the UAE (CBUAE) requires each LFI to take the necessary action to ensure protection of their systems against cyber threats. In case of any identified compromise, immediately contact CBUAE via infosec.bsd@cbuae.gov.ae.

Yours sincerely,

Ahmed Saeed Al Qamzi
Assistant Governor for Banking and Insurance Supervision
Encl:

مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Multiple Critical Vulnerabilities in Tridium Niagara Framework

Tracking #:432317543

Date:28-07-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple critical vulnerabilities in the Tridium Niagara Framework that could be exploited for remote code execution, compromise of credentials, and persistent backdoor access, potentially leading to full system takeover.

TECHNICAL DETAILS:

Multiple critical vulnerabilities exist in Tridium's **Niagara Framework**, a widely deployed platform in building automation, industrial control systems, and smart infrastructure. These vulnerabilities, if **misconfiguration disables encryption**, could allow attackers with network access to **compromise Niagara-based systems**, potentially resulting in **root-level remote code execution**, **lateral movement**, and **persistent access**.

Key Vulnerabilities
The most severe vulnerabilities include:

CVE	CVSS	Description
CVE-2025-3936	9.8	Incorrect Permission Assignment for Critical Resource
CVE-2025-3937	9.8	Use of Password Hash With Insufficient Computational Effort
CVE-2025-3938	9.8	Missing Cryptographic Step
CVE-2025-3941	9.8	Improper Handling of Windows: DATA Alternate Data Stream
CVE-2025-3944	9.8	Incorrect Permission Assignment for Critical Resource
CVE-2025-3945	9.8	Improper Neutralization of Argument Delimiters in a Command
CVE-2025-3943	7.3	Use of GET Request Method With Sensitive Query Strings

Exploit Chain:
An attack chaining **CVE-2025-3943** and **CVE-2025-3944**, enabling an attacker in a **Man-in-the-Middle (MitM)** position to:

1. **Steal an anti-CSRF token** from unencrypted logs via the Syslog service.
2. Use the token in a **Cross-Site Request Forgery (CSRF)** attack to force HTTP request logging.
3. Extract the admin session cookie (**JSESSIONID**) from the logs.
4. **Hijack the admin session**, create a new backdoor admin account.
5. **Download the TLS private key** and perform Adversary-in-the-Middle (AitM) attacks.
6. Trigger **remote code execution with root privileges** via CVE-2025-3944.

Successful exploitation of this vulnerabilities can lead to:

- Full compromise of Niagara system
- Unauthorized admin access and persistence
- Possible access to critical building and industrial controls
- Threat to safety, operations, and IT/OT network segmentation

Affected Product:

- **Tridium Niagara Framework**
- Impacted versions: prior to **4.14.2u2**, **4.15u1**, and **4.10u11**

RECOMMENDATIONS:

- Immediately apply all available security patches.
- Verify that encryption is enabled across all network communications.
- Review and enforce hardening guidelines, especially those related to logging, permissions, and remote access.
- Monitor dashboards for misconfiguration warnings, especially regarding encryption.
- Conduct network segmentation and restrict access to Niagara-connected devices.

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://www.nozominetworks.com/blog/critical-vulnerabilities-found-in-tridium-niagara-framework
- https://www.honeywell.com/us/en/product-security#security-notices

مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

High-Severity Vulnerabilities in Tableau Server

Tracking #:432317544

Date:28-07-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

ADVISORY

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

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

مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Authentication Bypass Vulnerability in Node-SAML

Tracking #:432317546

Date:28-07-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Node-SAML that could potentially be exploited to bypass authentication controls in affected systems.

TECHNICAL DETAILS:

A critical vulnerability exists in **Node-SAML**, a widely used open-source library that enables **SAML 2.0** authentication in Node.js applications. Tracked as **CVE-2025-54369**, this flaw undermines the trust model of SAML authentication and exposes millions of users to risk, including **privilege escalation**, **account confusion**, and **SSO bypasses**.

Vulnerability Details:

- **CVE-2025-54369**
- CVSS Score 9.3 Critical
- The issue stems from how Node-SAML **processes SAML responses**. While the library **correctly verifies XML signatures**, it subsequently **parses the assertion data from the original, unsigned document** instead of the validated content.
- Node-SAML loads the assertion from the (unsigned) original response document. This is different than the parts that are verified when checking signature.
- This **discrepancy opens the door for attackers** to alter critical authentication data—such as usernames—in the SAML assertion **after the signature has been verified**, bypassing standard authentication controls.
- **Exploitation of this vulnerability can lead to:**
  - **Privilege Escalation:** Impersonate admin or privileged accounts
  - **Account Confusion:** Misroute users or trigger policy mismatches
  - **SSO Bypass:** Circumvent checks by the Identity Provider (IdP)

Affected Versions:

- All versions of Node-SAML prior to 5.1.0

Fixed Versions:

- Node-SAML 5.1.0 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Node-SAML.

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://github.com/node-saml/node-saml/security/advisories/GHSA-m837-g268-mmv7