مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerabilities in TeamViewer DEX

Tracking #:432318177

Date:25-12-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that TeamViewer has released security updates addressing multiple high-severity vulnerabilities in its Digital Employee Experience (DEX) product suite (formerly 1E).

TECHNICAL DETAILS:

TeamViewer has released security updates addressing multiple high-severity vulnerabilities in its Digital Employee Experience (DEX) product suite (formerly 1E).The identified flaws impact both the DEX Windows Client and the DEX Platform (SaaS & On-Premise).

Vulnerability Breakdown:

1. Arbitrary Code Execution – Content Distribution Service
CVE-2025-44016
   - Severity: High
   - CVSS: 8.8

2. Denial of Service (Application Crash)
CVE-2025-12687
   - Severity: Medium
   - CVSS: 6.5

3.Information Disclosure / Data Leak
CVE-2025-46266
   - Severity: Medium
   - CVSS: 4.3

4. Command Injection – DEX Platform Instructions
CVE-2025-64986 – CVE-2025-64989
   - Severity: High
   - CVSS: 7.2

5. Local Privilege Escalation (SYSTEM)
CVE-2025-64994, CVE-2025-64995
   - Severity: High

Affected products & versions

- TeamViewer (1E) DEX Platform: SaaS< 25.12
- TeamViewer (1E) Platform: On-Premise All

RECOMMENDATIONS:

- Organizations are strongly advised to review the official TeamViewer security advisory in detail and promptly apply all applicable updates and mitigations for the TeamViewer Digital Employee Experience (DEX) platform and client components.

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.teamviewer.com/en/resources/trust-center/security-bulletins/tv-2025-1006/