Vulnerability Assessment Report Template

Ime i prezime: Aleksandar Sinđelić R2 14/2025
Tim: Kragujevac
Datum: 4.12.2025.
Scan Tool: OpenVAS (Greenbone OS 24.10.6)
Test okruženje: Metasploitable3

1. Enumeracija CVE-a

- **CVE ID: CVE-2025-3200**

- **Opis:**
  Neautentifikovani napadač može iskoristiti nebezbedne TLS 1.0 i TLS 1.1 protokole da presretne i manipuliše podacima na komunikaciji između Com Servera proizvođača Wiesemann & Theis i povezanih sistema.

---

2. CVSS skor

- **CVSS skor (numerička vrednost): 9.1 Critical**
- **Vektor:** `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N`

  - Attack Vector: Network
  - Attack Complexity: Low
  - Privileges Required: None
  - User Interaction: None
  - Scope: Unchanged
  - Confidentiality: High
  - Integrity: High
  - Availability: None

- **Opravdanje:**

Ranjivost ima visoku ocenu zato što omogućava udaljenim, neautentifikovanim napradačima da presretnu i menjaju šifrovane podatke uz malu kompleksnost.

---

3. Dostupnost eksploita

- **Postoji javno dostupan eksploit (Da/Ne):**
  Ne
- **Opis eksploita:**

- **Kod eksploita (ukoliko postoji):**

---

4. Analiza uzroka (root cause)

- **Uvođenje Greške (Commit/Verzija):**

  Com Serveri pre verzije 1.6 su konfigurisani da podržavaju metode šifrovanja koji su izloženi slabosti CWE-327

- **Primer Koda (ako je primenljivo):**

  U ovom slučaju nije navedeno koja metoda šifrovanja je dostupna ali primeri nekih takvih metoda su DES i RC4.

---

5. Preporuke za mitigaciju

- **Da li je dostupan Vendor Fix ili patch (Da/Ne): DA**
- **Mitigation Strategy:**
  Potrebno je ažurirati firmver na verziju 1.60 ili noviju.

6. Izvori

https://nvd.nist.gov/vuln/detail/cve-2025-3200
https://github.com/advisories/GHSA-9mjj-hhq6-4wp3
https://certvde.com/en/advisories/VDE-2025-031/
https://cwe.mitre.org/data/definitions/327.html