مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# High-Severity Vulnerabilities in BeyondTrust Privilege Management for Windows

Tracking #:432317556
Date:31-07-2025

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple high-severity vulnerabilities in BeyondTrust Privilege Management for Windows. These flaws could allow attackers to gain elevated privileges and disable endpoint protections, posing a serious risk to enterprise environments.

## TECHNICAL DETAILS:

**Vulnerability Details**:

- **CVE-2025-2297** – Local Elevation via User Profile Manipulation
  - **CVSS Score:** 7.2 (High)
  - A local authenticated attacker can manipulate user profile files to inject unauthorized challenge-response entries into the Windows registry. If the system is configured to auto-approve such challenges, this can result in privilege escalation to administrator level.

- **CVE-2025-6250** – Anti-Tamper Bypass via WMIC Exploit
  - **CVSS Score**: 7.1 (High)
  - Attackers with elevated privileges can exploit wmic.exe to stop the Defendpoint service, bypassing anti-tamper protections. This allows them to add themselves to the Administrators group and execute processes with elevated permissions.

**Affected Versions:**

- All versions prior to 25.4.270.0

**Fixed Versions:**

- 25.4.270.0 and later

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the latest updates released by BeyondTrust at the earliest.

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.beyondtrust.com/trust-center/security-advisories/bt25-05
- https://www.beyondtrust.com/trust-center/security-advisories/bt25-06