مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – TrendMicro WFBSS
Tracking #:432317483
Date:14-07-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that TrendMicro released a security advisory addressing multiple vulnerabilities in its Worry-Free Business Security Services (WFBSS) agent.

TECHNICAL DETAILS:

TrendMicro released a security advisory addressing multiple vulnerabilities in its Worry-Free Business Security Services (WFBSS) agent. These vulnerabilities if left unpatched could allow an attacker to gain remote control, execute arbitrary code, or compromise system stability.

Vulnerability Details:
- **CVE-2025-49154**: Insecure Access Control Vulnerability
- **CVSSv3.1:** 8.7 - High
- **Weakness:** CWE-284: Improper Access Control
- **Description**: An insecure access control vulnerability in Trend Micro Worry-Free Business Security and Worry-Free Business Security Services could allow a local attacker to overwrite key memory-mapped files which could then have severe consequences for the security and stability of affected installations.

- **CVE-2025-53378**: Missing Authentication Vulnerability
- **CVSSv3.1:** 7.6 - High
- **Weakness:** CWE-306: Missing Authentication for Critical Function
- **Description**: A missing authentication vulnerability in Trend Micro Worry-Free Business Security Services (WFBSS) agent could have allowed an unauthenticated attacker to remotely take control of the agent on affected installations.
- **Note:** This vulnerability affected only the SaaS version of WFBSS; the on-premises version was not impacted. It was resolved in a monthly maintenance update, and no further action is required if agents follow the regular SaaS deployment schedule. This disclosure is for informational purposes only.

- **CVE-2025-49487**: Uncontrolled Search Path Element Arbitrary Code Execution Vulnerability
- **CVSSv3.1:** 6.8 - Medium
- **Weakness:** CWE-427: Uncontrolled Search Path Element
- **Description**: An uncontrolled search path vulnerability in the Trend Micro Worry-Free Business Security Services (WFBSS) agent could have allowed an attacker with physical access to a machine to execute arbitrary code on affected installations.

Affected Versions:
- Worry-Free Business Security (WFBS) - 10.0 SP1
- Worry-Free Business Security Services (WFBSS) - 6.7 (SaaS)

Fixed Versions:
- WFBS - 10 SP1 Patch 2514
- WFBSS - May 2025 Monthly Release - (6.7.3954 / 14.3.1299)

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to immediately apply the latest patches for the Worry-Free Business Security Services (WFBSS) agent.

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://success.trendmicro.com/en-US/solution/KA-0019936

TLP: WHITE