مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates-ASUS Business Manager

Tracking #:432318342

Date:03-02-2026

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

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed ASUS has released a mandatory security update for ASUS Business Manager, an enterprise administration utility used on ASUS commercial computers to manage system configuration, data protection, and encrypted partitions.

TECHNICAL DETAILS:

ASUS has released a mandatory security update for ASUS Business Manager, an enterprise administration utility used on ASUS commercial computers to manage system configuration, data protection, and encrypted partitions. The update addresses a high-severity local privilege escalation (LPE) vulnerability identified as CVE-2025-13348, affecting the Secure Delete / File Shredder driver. Due to improper access control enforcement, a local attacker could exploit the vulnerable driver to perform arbitrary file creation, potentially leading to full system compromise.
Rather than patching the vulnerable component, ASUS has permanently removed the File Shredder feature in version 3.0.37.0, eliminating the attack surface entirely.

Vulnerability Details:

- CVE ID: **CVE-2025-13348**
- Severity: High
- CVSS v4.0 Score: 8.5
- Attack Vector: Local
- Impact Type: Privilege Escalation / Arbitrary File Creation

Affected Component

- ASUS Secure Delete Driver
- Feature exposed through File Shredder functionality in ASUS Business Manager

Root Cause

- Improper access control (authorization bypass) within the Secure Delete kernel-level driver
- Insufficient validation of user-supplied requests sent to the driver

Exploitation Scenario

A local attacker with limited privileges could:

- Send specially crafted IOCTL requests to the Secure Delete driver
- Instruct the driver to create arbitrary files at attacker-controlled paths

Fixed Versions:

- ASUS Business Manager version 3.0.37.0 or later

RECOMMENDATIONS:

- Upgrade ASUS Business Manager to fixed version immediately.

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.asus.com/security-advisory/