Posting Date: 2026/09/10

【Vulnerability Alert】Sunsea Information【SmartIT Desktop Manager - Presence of 2 Critical Security Vulnerabilities

- Subject: 【Vulnerability Alert】Sunsea Information【SmartIT Desktop Manager - Presence of 2 Critical Security Vulnerabilities

- Description:
  - Forwarding Taiwan Computer Emergency Response Team / Coordination Center Cybersecurity Alert TWCERTCC-200-202609-00000006
  - Sunsea Information product SmartIT Desktop Manager has 4 security vulnerabilities, including 2 critical security vulnerabilities:
  - 【Sunsea Information】SmartIT Desktop Manager - Use of Hard-coded Credentials【(CVE-2026-85146, CVSS: 9.8) Unauthenticated remote attackers can obtain the SSH service account and password for the SmartIT Agent program within the code.
  - 【Sunsea Information】SmartIT Desktop Manager - Use of Hard-coded Credentials【(CVE-2026-85147, CVSS: 7.5) Unauthenticated remote attackers can obtain a specific password within the code, which can be used to acquire the AES encryption key for communication.
  - 【Sunsea Information】SmartIT Desktop Manager - Use of Hard-coded Credentials【(CVE-2026-85148, CVSS: 9.8) Unauthenticated remote attackers can use a fixed password to remotely access user hosts.
  - 【Sunsea Information】SmartIT Desktop Manager - Use of Hard-coded Credentials【(CVE-2026-85149, CVSS: 5.3) Unauthenticated remote attackers can obtain the SFTP service account and password for the SmartIT Agent program within the code, thereby browsing the user host file system.
- Affected Platforms:
  - SmartIT Desktop Manager version 10 (inclusive) and earlier versions
- Recommended Actions:
  - Update to SmartIT Desktop Manager version 11 (inclusive) and later versions
- References:
  1. https://www.twcert.org.tw/tw/cp-132-11176-a4cc2-1.html

Computer and Communication Center
Network System Division

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260910_21

Last update: **2026/09/10 16:18**