Posting Date: 2026/07/17

【Vulnerability Alert】SAP Releases Major Security Advisories for Multiple Products

- Subject: 【Vulnerability Alert】SAP Releases Major Security Advisories for Multiple Products

- Description:
  - Forwarded from the Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) security alert TWCERTCC-200-202607-00000008.
  - 【CVE-2026-44747, CVSS: 9.9】 SAP NetWeaver Application Server ABAP allows an authenticated attacker to exploit a logic error in memory management to cause memory corruption, leading to unauthorized data access, modification, or system unavailability.
  - 【CVE-2026-27690, CVSS: 9.1】 An HTTP Request Smuggling vulnerability exists in SAP Approuter. An unauthenticated attacker can send specially crafted HTTP requests, leading to request-response desynchronization, which may leak user response data and result in system unavailability.
  - 【CVE-2026-44761, CVSS: 9.1】 SAP Commerce Cloud may retain sample OAuth2 clients containing publicly documented sample credentials, which originate from sample configurations provided in the SAP Help Portal documentation. An unauthenticated attacker can exploit these public credentials to obtain valid tokens and call certain APIs to read and modify data.
- Affected Platforms:
  - SAP NetWeaver Application Server ABAP Version(s) - KRNL64NUC 7.22, 722EXT, KRNL64UC 7.22, 7.22EXT, 7.53, KERNEL 7.22, 7.53, 7.54, 7.77, 7.89, 7.93, 9.16, 9.18, 9.19, 9.20
  - SAP Approuter Version(s) - SAP Approuter node.js package 20.10.0
  - SAP Commerce Cloud Version(s) - HY_COM 2205, COM_CLOUD 2211, 2211-JDK21
- Recommended Actions:
  - Apply patches according to the solutions released on the official website: https://support.sap.com/en/my-support/knowledge-base/security-notes-news/july-2026.html

---

Computer and Communication Center
Network Systems Division Sincerely

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

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260717_23

Last update: **2026/07/17 11:16**