```` **Posting Date: 2026/08/17**

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

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

- Description:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center Security Alert TWCERTCC-200-202608-00000010
  - SAP has released its August routine security updates, which include 4 high-risk vulnerabilities.
  - 【CVE-2026-58231, CVSS: 10.0】 SAP Commerce Cloud allows an unauthenticated attacker to abuse default authentication clients and submit specially crafted input to certain functions that lack full validation. Successful exploitation of this vulnerability could lead to arbitrary code execution and compromise internal components.
  - 【CVE-2026-34265, CVSS: 9.8】 SAP NetWeaver and ABAP Platform allow an unauthenticated attacker to exploit a logic flaw in DIAG protocol parsing, which may lead to memory corruption, disclosure of sensitive system information, or system crash.
  - 【CVE-2026-44758, CVSS: 9.1】 SAP Manufacturing Integration and Intelligence allows a highly privileged attacker to submit specially crafted input to certain affected functions without sufficient validation. Successful exploitation of this vulnerability enables the attacker to execute arbitrary commands on the underlying operating system.
  - 【CVE-2026-58243, CVSS: 8.8】 Certain functions in SAP ABAP Developer Tools fail to perform necessary authorization checks, allowing a low-privileged attacker to execute unauthorized database operations on SAP NetWeaver AS ABAP. Successful exploitation of this vulnerability could allow the attacker to read sensitive data, modify application data, and disrupt access for legitimate users.
- Affected Platforms:
  - 【CVE-2026-58231】 SAP Commerce Cloud (Data Hub Adapter) Version(s) - COM_CLOUD 2211, 2211-JDK21
  - 【CVE-2026-34265】 SAP NetWeaver and ABAP Platform Version(s) - KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT, 7.22EXT2, 7.22EXT3, 7.53, 7.54, 7.77, 7.89, 7.93, 8.04, 9.16 9.18, 9.19, KERNEL 7.22, 7.53, 7.54, 7.77, 7.89, 7.93, 8.04, 9.16, 9.18, 9.19
  - 【CVE-2026-44758】 SAP Manufacturing Integration and Intelligence Version(s) - XMII 15.4, 15.5
  - 【CVE-2026-58243】 SAP ABAP Developer Tools Version(s) - SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 816, SAP_BASIS 918, SAP_BASIS 920
- Recommendations:
  - Apply patches according to the solution released on the official website: https://support.sap.com/en/my-support/knowledge-base/security-notes-news/august-2026.html?isu_page=1
- References:
  1. https://www.twcert.org.tw/tw/cp-169-11102-6a741-1.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:20260817_22**

Last update: **2026/08/17 16:07**
```