Date Posted: 2026/06/15

Vulnerability Alert SAP Issues Major Security Advisories for Multiple Products

- Subject: Vulnerability Alert SAP Issues Major Security Advisories for Multiple Products

- Description:
  - Forwarded from Taiwan Computer Emergency Response Team / Coordination Center Security Advisory TWCERTCC-200-202606-00000009
  - CVE-2026-40128, CVSS: 9.0 SAP NetWeaver Application Server Java (Web Container) allows unauthenticated attackers to trigger path traversal behavior via crafted HTTP login requests.
  - CVE-2026-27671, CVSS: 9.8 Due to insufficient validation of the RFC protocol used by SAP NetWeaver AS ABAP and ABAP Platform, unauthenticated attackers can exploit memory logic errors to cause corruption via crafted RFC requests.
  - CVE-2026-44748, CVSS: 9.9 SAP NetWeaver AS ABAP and ABAP Platform allow authenticated attackers with standard privileges to obtain a validly signed message, tamper with the content of the signed document, and submit it to the validator.
- Affected Platforms:
  - SAP NetWeaver AS ABAP and ABAP Platform Version(s) - KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 722EXT, 7.53, KERNEL 7.22, 7.53, 7.54, 7.77, 7.89, 7.93, 9.16, 9.18, 91.9
  - SAP NetWeaver AS ABAP and ABAP Platform Version(s) - SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, 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 919
  - SAP NetWeaver Application Server Java (Web Container) Version(s) - ENGINEAPI 7.50
- Recommended Actions:
  - Apply patches according to the solution released on the official website: https://support.sap.com/en/my-support/knowledge-base/security-notes-news/june-2026.html
- References:
  1. https://www.twcert.org.tw/tw/cp-169-10963-9280d-1.html

Computer and Communication Center
Network Systems Division