CYBER ADVISORY

Thursday, June 11, 2026 **CAL-CSIC-202606-A-006**

Multiple Vulnerabilities Impacting SAP Products

Improper Verification	Stack-Based Buffer Overflow	Path Traversal	Patches Available

The Cybersecurity Integration Center (CSIC) has become aware of a trio of critical-severity vulnerabilities impacting SAP products. CVE-2026-44748 and CVE-2026-27671 impact SAP NetWeaver Application Server ABAP (Advanced Business Application Programming), while CVE-2026-40128 impacts SAP NetWeaver Application Server Java (Web Container). CVE-2026-44748 carries a CVSS 3.1 score of 9.9[1], while CVE-2026-27671 carries a CVSS 3.1 score of 9.8.[2] CVE-2026-40128 carries a CVSS 3.1 score of 9.0.[3]

CVE-2026-44748 is an Improper Verification of Cryptographic Signature vulnerability and impacts the SAP NetWeaver Application Server ABAP. It enables an attacker to intercept or obtain a validly signed SAML (Security Assertion Markup Language) message to manipulate the underlying XML payload, and present modified information to the verifier. Successful exploitation allows the attacker to bypass authentication boundaries, hijack identities, escalate privileges, and gain unrestricted admin access to sensitive user data.[4]

CVE-2026-27671 is a Stack-based Buffer Overflow vulnerability and also impacts the SAP NetWeaver Application Server ABAP platform. However, this vulnerability is rooted in the improper RFC (Remote Function Call) protocol validation within the SAP kernel used by Application Server ABAP. It allows an unauthenticated remote attacker to issue a specifically crafted RFC request designed to exploit logical errors in memory management. Successful exploitation triggers memory corruption and provides a direct vector for remote code execution at the system level on the targeted device.[5]

CVE-2026-40128 is a Path Traversal vulnerability that targets the SAP NetWeaver Application Server Java Web Container. The vulnerability allows an unauthenticated attacker to craft a malicious HTTP logon request that manipulates file inclusion parameters. Successful exploitation results in the web container processing the malicious file - exposing sensitive data, allowing file modification and deletion, or cause a denial of service. The vulnerability does not require authentication, therefore any external user with network access could target the system.[6]

Individually, successful exploitation of these vulnerabilities would directly impact an organization's confidentiality, integrity, and availability of the target Application Server. This trio of vulnerabilities are not currently being exploited as zero-day exploits, nor is there confirmation of exploitation in the wild. Additionally, there are not publicly available Proof-of-Concepts for these vulnerabilities at the time of the writing of this advisory. SAP has issued patches for each of these vulnerabilities as part of their monthly patch day for June.[7]

The Cal-CSIC recommends following SAP's guidance for patching these three vulnerabilities. To review SAP's technical details, please use these links:

https://support.sap.com/en/my-support/knowledge-base/security-notes-news/june-2026.html

https://me.sap.com/app/securitynotes (*requires SAP account and login*)

Affected Product(s) and Version(s)

CVE	Product	Version
CVE-2026-44748	NetWeaver Application Server ABAP	(SAP_BASIS) 702, 731, 740, 750 751, 752, 753, 754 755, 756, 757, 758 816, 918, 919
CVE-2026-27671	SAP NetWeaver Application Server ABAP and ABAP Platform	KRNL64NUC 7.22 7.22EXT KRNL64UC 7.22 722EXT 7.53 KERNEL 7.22 7.54, 7.77, 7.89, 7.93 9.16, 9.18, 91.9
CVE-2026-40128	SAP NetWeaver Application Server Java (Web Container)	ENGINEAPI 7.50

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: California Cybersecurity Integration Center | California Governor's Office of Emergency Services

References

[1] NVD; "CVE-2026-44748 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2026-44748; accessed 09 June 2026
[2] NVD; "CVE-2026-27671 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2026-27671; accessed 09 June 2026
[3] NVD; "CVE-2026-40128 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2026-40128; accessed 09 June 2026
[4] OpenCVE; "CVE-2026-44748"; https://app.opencve.io/cve/CVE-2026-44748; accessed 09 June 2026
[5] OpenCVE; "CVE-2026-27671"; https://app.opencve.io/cve/CVE-2026-27671; accessed 09 June 2026
[6] OpenCVE; "CVE-2026-40128"; https://app.opencve.io/cve/CVE-2026-40128; accessed 09 June 2026
[7] SAP Support; "SAP Security Patch Day – June 2026"; https://support.sap.com/en/my-support/knowledge-base/security-notes-news/june-2026.html; accessed 09 June 2026