Race Against Hackers: SecurityBridge Discovers Near Maximum-Severity 9.9 out of 10 SAP Vulnerability

NEW YORK, NY, UNITED STATES, November 11, 2025 /EINPresswire.com/ -- SecurityBridge, creator of the Cybersecurity Command Center for SAP, today announced that the SecurityBridge Threat Research Labs uncovered a critical SAP vulnerability rated a 9.9 out of 10 severity, and gave its customers advanced notice on October 30, 2025, to update detection signatures before the vulnerability was publicly disclosed.

In total, the Threat Research Labs uncovered three vulnerabilities that were among the 25 new and updated SAP Security Notes SAP published today for its November Patch Day. Contained in the SAP Patch Day alert, the HotNews note 3668705 – [CVE-2025-42887] Code Injection vulnerability in SAP Solution Manager describes how a remote-enabled function module can be misused to inject malicious code, resulting in complete system control. A public patch for this vulnerability has been released today, which might speed up reverse-engineering and exploit development, so patching soon is advised.

In addition to the highest priority category discovered, the Threat Research Labs found the following two vulnerabilities, also released within the SAP Patch Day notes:

-Medium priority: note 3643337 – [CVE-2025-42882] Missing Authorization check in SAP NetWeaver Application Server for ABAP 4.3.

-Low priority: note 3634053 – [CVE-2025-42883] Insecure File Operations vulnerability in SAP NetWeaver Application Server for ABAP (Migration Workbench).

"When we discover a vulnerability that scores a 9.9 out of 10 priority rating, we know we're looking at a threat that could give attackers complete system control," said Joris van de Vis, Director of Security Research, SecurityBridge. "CVE-2025-42887 is particularly dangerous because it allows to inject code from a low-privileged user, which leads to a full SAP compromise and all data contained in the SAP system. This code-injection vulnerability in SAP Solution Manager represents exactly the kind of critical attack surface weakness that our Threat Research Labs work tirelessly to identify and eliminate. SAP systems are the backbone of business operations, and vulnerabilities like this remind us why proactive security research is non-negotiable."

The SecurityBridge Threat Research Labs has a history of uncovering the most critical SAP vulnerabilities:

-In September 2025, the company discovered a Critical SAP S/4HANA code injection vulnerability (CVE-2025-42957), rated 9.9 out of 10 in severity.

-In August 2025, the team discovered three vulnerabilities, two of which were rated 9.9 out of 10 in severity: [CVE-2025-42950] Code Injection Vulnerability in SAP Landscape Transformation (Analysis Platform), [CVE-2025-42957] Code Injection vulnerability in SAP S/4HANA (Private Cloud or On-Premise) and [CVE-2025-42946] Directory Traversal vulnerability in SAP S/4HANA (Bank Communication Management).

The company has updated the SecurityBridge Platform to ensure customers are insulated from known vulnerabilities. SecurityBridge's Patch Management offers invaluable insights into existing patching gaps within SAP landscapes, a complete list of todayś new vulnerabilities, and an overview. Please visit: https://securitybridge.com/blog/sap-security-patch-day-november-2025/.

Betsey Rogers
Bridgeview Marketing
betsey@bridgeviewmarketing.com
Visit us on social media:
LinkedIn
X