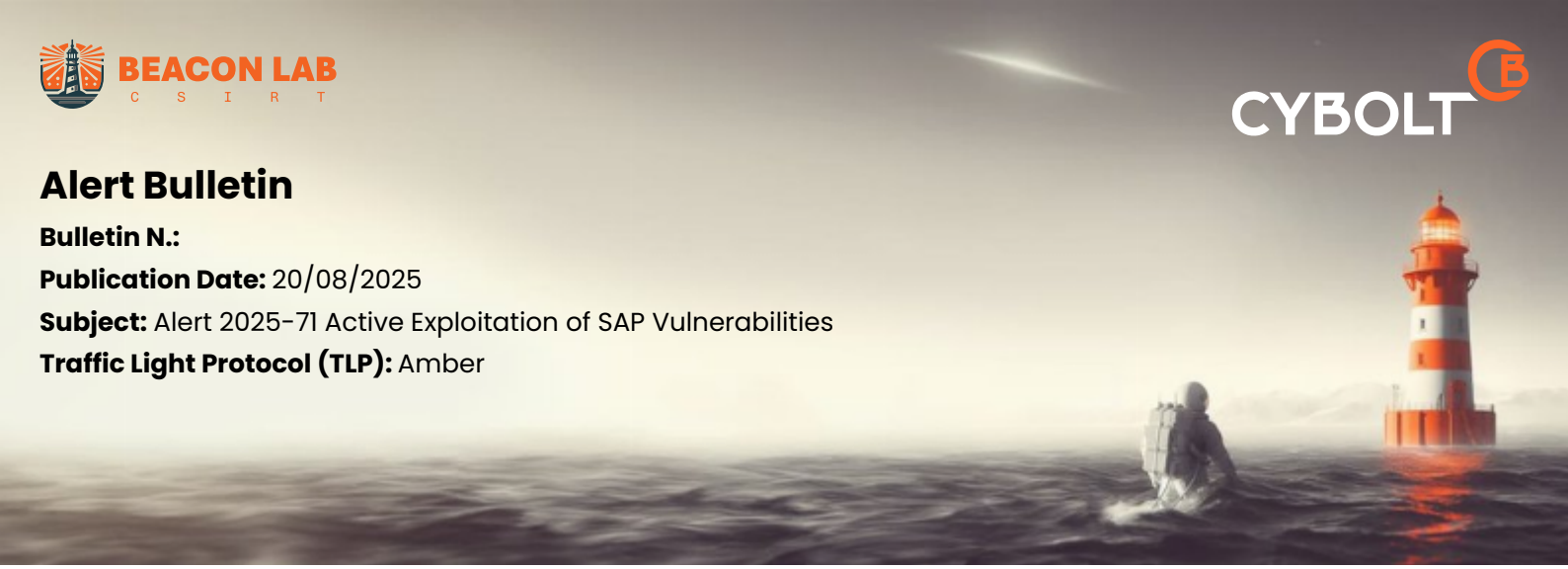

Alert Bulletin

Bulletin N.:
Publication Date: 20/08/2025
Subject: Alert 2025-71 Active Exploitation of SAP Vulnerabilities
Traffic Light Protocol (TLP): Amber

Affected product(s):

- SAP Netweaver 7.50
- SAP Netweaver 7.5

Descripción

Two critical flaws have been identified in SAP NetWeaver Visual Composer that, although they already have official patches, are currently being actively exploited by different threat actors.

The first vulnerability, registered as **CVE-2025-31324** and with a CVSS score of 10.0, corresponds to a lack of authorization check. This flaw allows an unauthenticated attacker to upload malicious files directly to the affected server, opening the door to a total compromise of the SAP system, affecting its confidentiality, integrity, and availability.

The second vulnerability, identified as **CVE-2025-42999** and with a CVSS score of 9.1, is related to an **insecure deserialization** process. In this case, a privileged user can upload malicious content that, when processed, is executed with elevated permissions. This allows attackers to take control of the system, execute remote code, and compromise both data and business-critical processes.

Currently, these vulnerabilities taken together are not merely theoretical; are **being actively exploited in real and targeted attacks** against organizations.

- **Ransomware on the Spread**

Groups such as **Qilin, BianLian, and RansomEXX** have incorporated these flaws into their campaigns. Its main purpose is **to disrupt business operations**, **encrypt critical data** , and **extort money from organizations** for ransom.
These groups are known for acting quickly and opportunistically: as soon as a new critical vulnerability emerges, they integrate it into their attacks to maximize the impact before companies apply patches.

- **Espionage campaigns**

In addition to ransomware operations, the use of these vulnerabilities by **threat actors linked to China**, focused on **critical infrastructure and strategic corporate networks**, has been identified. In this context, the objective is not necessarily economic, but the **theft of sensitive information** for industrial espionage purposes.

- **Advanced attack tactics**

The exploit allows not only the installation of webshells to maintain remote access, but also the use of "Living off the Land" (LotL) techniques. This means that attackers can execute commands directly into the operating system using legitimate SAP or system tools, reducing the likelihood of being detected by traditional security solutions.

Solution:

Immediately update devices to the **most current** version

Additional information:

- https://thehackernews.com/2025/08/public-exploit-for-chained-sap-flaws.html
- https://reliaquest.com/blog/threat-spotlight-reliaquest-uncovers-vulnerability-behind-sap-netweaver-compromise/
- https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html

  https://accounts.sap.com/saml2/idp/sso