Health-ISAC
Collaborating for Resilience in Health

THREAT BULLETINS

Critical SAP S/4HANA Vulnerability Actively Exploited (CVE-2025-42957)

TLP:WHITE

Sep 09, 2025

Exploitation of the SAP S/4HANA flaw, tracked as CVE-2025-42957, has been disclosed. The vulnerability allows code injection and privilege escalation, potentially giving a low-privileged user full control of the SAP system.

The flaw, originally disclosed and patched in August, has a CVSS score of 9.9, highlighting its criticality. It affects all S/4 HANA releases, including Private Cloud and On-Premise.

An attacker only needs a valid SAP user account with access to a specific vulnerable RFC module and the S_DMIS authorization object. No user interaction, such as clicking a malicious link, is required. This low bar for entry makes the attack particularly dangerous.

Once an attacker gains a foothold, they can execute arbitrary ABAP code, read or modify any data, create new administrative users, steal password hashes, and disrupt critical business processes.

The exploit's simplicity and network-based nature allow a threat actor to quickly escalate basic user credentials obtained through phishing or an insider threat into a full compromise of the entire SAP environment.

Recommendations:

- Patch all vulnerable SAP S/4HANA instances.
- Enforce network segmentation and strict network access control policies.
- Implement multi-factor authentication for accounts across the organization.
- Continuously monitor for suspicious activities, including unauthorized access and unusual appliance logs or connections.
- Have an incident response plan ready to limit operational disruptions in the event of a successful attack.
- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients resources.

Reference(s)	gbhackers, securitybridge, pathlock, hhs

Sources
https://securitybridge.com/blog/critical-sap-s-4hana-code-injection-vulnerability-cve-2025-42957/

https://gbhackers.com/critical-sap-s-4hana-vulnerability/

https://pathlock.com/blog/security-alerts/cve-2025-42957-critical-sap-s-4hana-code-injection-vulnerability/

Incident Date
Sep 08, 2025 (UTC)

Alert ID e4704575

View Alert

Share Feedback

was this helpful? |

Tags CVE-2025-42957, SAP S/4HANA

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**