



Quarterly Report

SecurityBridge Research Labs

Update Q3 2025

Advancing SAP Security Through Innovation

The [SecurityBridge Research Lab](#) is at the forefront of SAP cybersecurity, driving innovation through advanced vulnerability research, collaborative disclosure, and cutting-edge product integration. By combining technical expertise with strong partnerships, the Lab continuously strengthens the resilience of SAP landscapes worldwide.

Our mission is clear: identify critical vulnerabilities, enable responsible remediation, and deliver research-driven solutions that empower organizations to protect their most vital business systems. All to make the world run more securely.

Importance of Security Research

Everybody benefits



SecurityBridge Customers

- Enhanced and broader threat detection
- Earlier identification - even before SAP releases a patch
- Minimized impact and reduced costs
- Automatic platform updates powered by insights from our security research team



All of SAP Customers

- Findings fixed by SAP and patched by customers cannot be abused by malicious actors, helping all customers in the SAP ecosystem
- Sharing is caring > growing awareness and active reaching out to vulnerable SAP customers, eg. by scanning for exposed systems through our own research and in collaboration with organizations like the Dutch Institute for Vulnerability Disclosure



The World

- SAP systems power critical industries - from governments to food production
- SAP customers drive 87% of global commerce (\$46 trillion)*
- 99 of the world's 100 largest companies rely on SAP*
- Securing SAP systems means protecting more than just revenue - it's about safeguarding global stability

[*View the SAP corporate fact sheet](#)

Key Achievements in Q3 2025

- **Strategic Collaboration:** In partnership with the Dutch Institute for Vulnerability Disclosure ([DIVD](#)), we led a global initiative to scan and notify system owners about exposure to [CVE-2025-31324](#), reducing the number of vulnerable SAP systems on the internet.
- **High-Impact Vulnerability Research:**
 - A total of **five SAP 0-day vulnerabilities** were responsibly disclosed and remediated by SAP, with CVSS scores ranging up to **9.9 (HotNews)**.
 - Discoveries spanned critical platforms including **SAP S/4HANA, SAP NetWeaver, and SAP Ariba**.
 - Our findings were consistently acknowledged by SAP, underscoring our Lab's credibility and contribution.
- **Immediate Security Relevance:** The release of a [public exploit](#) by the **Lapsus hacking group** shortly after [our CVE-2025-31324 scanning](#) campaign highlights the real-world urgency and [impact](#) of our proactive efforts.

Highlights of Reported Vulnerabilities

In Q3 of 2025, SAP patched a total of 5 vulnerabilities discovered by the SecurityBridge Research Lab:

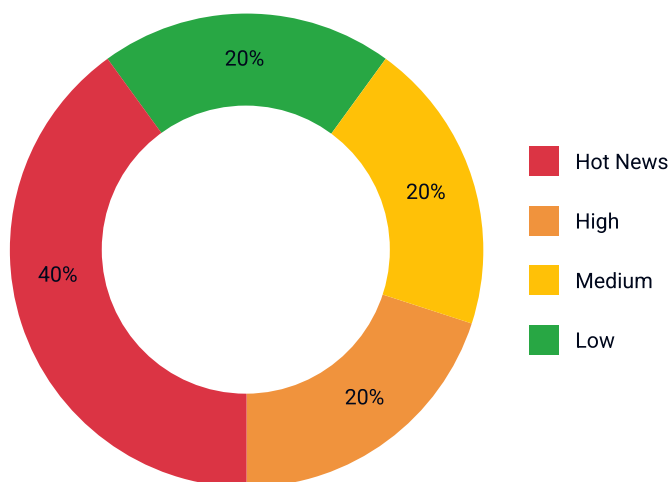
Note	CVE	Description	Severity	CVSS	Month Fixed	Platform
3608156	CVE-2025-42954	DoS in SAP NetWeaver Business Warehouse (CCAW)	Low	2.7	Jul 2025	NetWeaver
3614804	CVE-2025-42946	Directory Traversal in S/4HANA (Bank Communication Mgmt)	Medium	6.9	Aug 2025	S/4HANA
Silently patched	Silently patched	Ariba API flaw - Authentication re-use	High	n.a	Aug 2025	Ariba
3627998	CVE-2025-42957	ABAP Code Injection in S/4HANA (Private Cloud / On-Prem)	HotNews	9.9	Aug 2025	S/4HANA
3623504	CVE-2025-42918	Missing Authorization in NetWeaver ABAP (Background Processing)	Medium	4.3	Sept 2025	NetWeaver

Special Note:

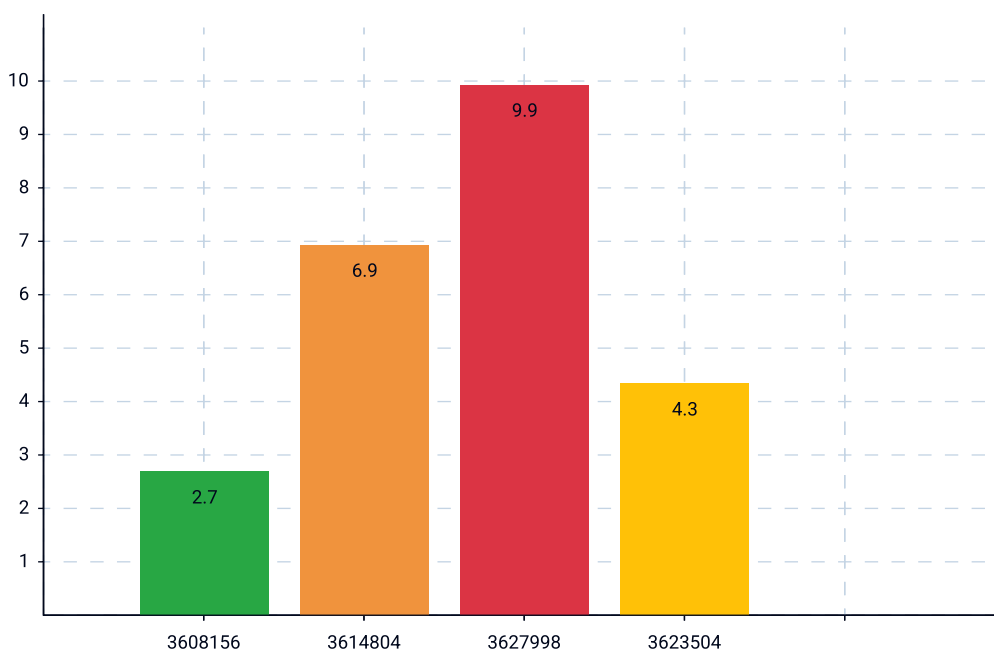
- **CVE-2025-42957** is a critical Remote Code Execution vulnerability, capable of compromising the entire SAP system. Exploitation could enable malware deployment, data theft, fraud, or operational disruption. SAP released a **HotNews patch** in August 2025, and our team delivered **Virtual Patching** capabilities in SecurityBridge products to protect customers during the remediation window. Find full details in our [blog post](#) and ensure timely patching where applicable.

A breakdown of the severity and the CVSS score is provided below:

Severity of findings reported by the SecurityBridge Research Labs



CVSS Scores of findings reported by the SecurityBridge Research Lab



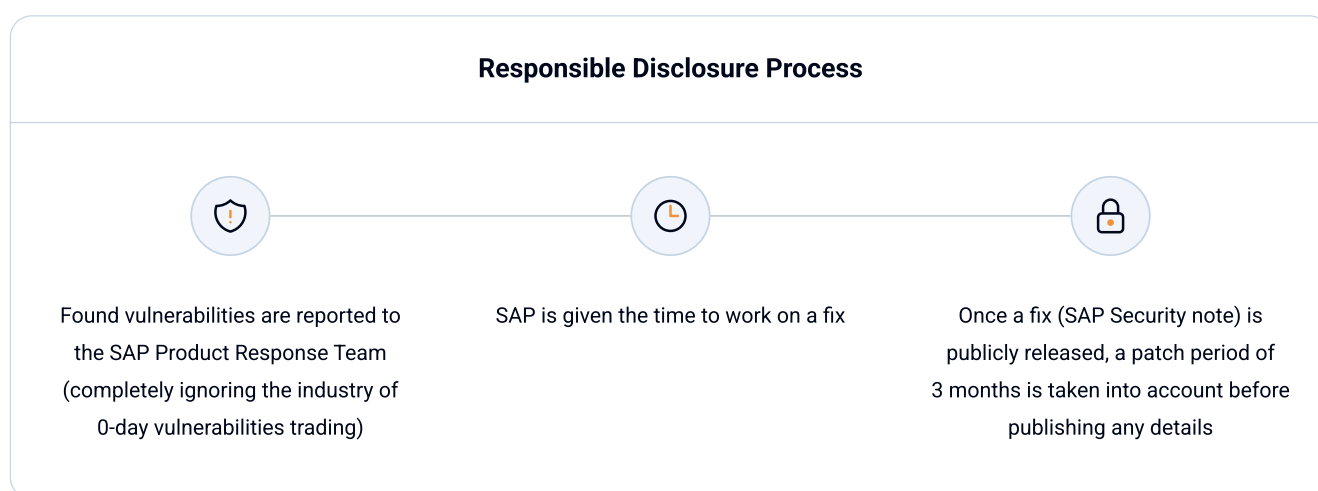
As we respect a grace period of 3 months to allow customers to implement the patches, full details about the vulnerabilities found cannot be shared yet. However, for some of the above-released patches, SecurityBridge has shipped product updates to detect execution of vulnerable ABAP programs via our Virtual Patching functionality.

How We Discover Vulnerabilities

The SecurityBridge Research Lab applies a multi-faceted methodology, combining:

- **Proprietary Tools** – to index, scan, and analyze large-scale SAP codebases.
- **Reverse Engineering** – uncovering hidden flaws in SAP components.
- **Design & Architecture Reviews** – exposing systemic weaknesses.
- **Practical Exploitation Testing** – validating real-world impact and eliminating false positives.

This rigorous approach ensures **accuracy, ethical compliance, and maximum-security value** for SAP customers.



Risk Assessment & Customer Protection

- All reported vulnerabilities require at least low-level authentication, with the majority enabling **privilege escalation**.
- The HotNews-class ABAP injection represents the highest risk, with the potential **for complete compromise of SAP systems and data**.
- To protect customers, **SecurityBridge Patch Management** integrates research-driven updates, enabling rapid identification and mitigation of emerging threats.

Recommendation: Organizations must apply the relevant SAP Security Notes promptly and leverage SecurityBridge’s integrated monitoring and patching capabilities.

Recognition & Acknowledgements

The contributions of our researchers continue to be recognized by SAP. In Q3, **Gert-Jan Koster** and **Chee-Lun Wong** received special acknowledgements for their discoveries, highlighting the talent and dedication within our Lab. Notably, our team has been consistently acknowledged every month throughout 2025.

How to protect yourself

To ensure protection against these and other vulnerabilities, it is essential to apply patches without delay and consider proper testing. The SecurityBridge Research Lab works closely with product development to deliver continuous updates – for example, through enhancement in the SecurityBridge Patch Management module. Make sure to identify relevant SAP Security notes for your SAP systems and apply them as soon as possible.

About SecurityBridge


SecurityBridge is the leading provider of a **comprehensive, SAP-native cybersecurity platform**, trusted globally to safeguard mission-critical business systems. With over **8,000 SAP systems secured** and a proven record of customer success, our platform delivers:


- Real-time **threat detection and monitoring**
- Integrated **vulnerability management**
- Automated **compliance and patch intelligence**

Through continuous innovation and **Research Lab insights**, SecurityBridge empowers organizations to achieve **full-spectrum SAP protection** with clarity, speed, and confidence.


Locations

Germany (Headquarters)

 Münchener Str. 49, 85051 Ingolstadt

 +49 (841) 93914840

Netherlands

 Kraijenhoffstraat 137A, 1018RG Amsterdam


 +31 647 100 101


United States

 228 Park Ave S, New York, New York

 +1 416 821 0850

Singapore

 4 Battery Road, Bank Of China Building, #25-01, Singapore (049908)

 +65 9126 6097

See SecurityBridge in Action

Reach out to us if you are ready to talk SAP security or want to see SecurityBridge in action.

[Request a demo](#)
[Contact Us](#)



For more information please contact

info@securitybridge.com

www.securitybridge.com