ONAPSIS

SAP® Endorsed App
Premium Certified

Executive Threat Overview: Critical Zero-Day SAP Vulnerabilities Under Active Global Exploitation

Executive Summary

Two critical SAP cybersecurity vulnerabilities are being actively exploited at least since March 12, 2025. These issues affect a component of the SAP NetWeaver Java Application Server, which supports critical business solutions such as SAP ERP, SCM, PI/PO, SRM, PLM, CRM, EP, BI/BW, HCM, and many others. While this component is fortunately not enabled by default, Onapsis Research Labs estimates that over 4,000+ of these systems were directly reachable over the Internet, and 50-70% of them had the vulnerable component present at the time this attack campaign began.

Intelligence reports indicate that hundreds of SAP systems have been compromised, and many still remain vulnerable today. Attacks are being performed by multiple threat actor groups, including China-nexus threat actors and Russia-linked ransomware groups, and are actively targeting SAP customers across different industries and geographies. Successful attacks result in full compromise of SAP applications, carrying significant operational, financial, regulatory and reputational risk for affected organizations. SAP responded quickly and released emergency critical patches on April 24, 2025, and May 13, 2025 to address the vulnerabilities. SAP, Onapsis, and global government agencies are urging SAP customers to take immediate action to protect their organizations.

What is the Business Risk?

By exploiting these vulnerabilities, unauthenticated threat actors can gain unrestricted remote access to SAP business-critical data and processes, including the ability to exfiltrate, modify, or delete confidential and/or regulated information as well as disrupt operations. Exploitation bypasses traditional SAP security controls (such as user access and segregation of duties) and may leave no traces in standard SAP application audit logs.

Business impact to affected organizations could be significant, including (but not limited to) critical service disruption; ransomware; unauthorized business activity (e.g., modifying financial records or fraudulent payments); theft of confidential, sensitive, & regulated information (e.g., PII, customer, or materials data); lateral movement to other critical internal systems; and non-compliance with regulations such as SOX, GDPR, HIPAA, NERC, NIS2 and others.

Key Challenges Requiring Immediate Attention

Onapsis notes three key challenges numerous organizations are still facing as this attack campaign continues:

1) **Many organizations still have vulnerable SAP systems connected to the internet today.**
Why? Cybersecurity teams may be unaware due to lacking visibility into SAP patches or critical alerts, mission-critical SAP applications may not have received the required downtime, and/or ineffective temporary mitigations may have been applied.

2) **Many organizations applied the SAP security patches or workarounds, but do not realize they have been already compromised.**
Why? SAP application owners may be unfamiliar with the concept of 'zero-day attacks': threat actors may have compromised their systems *before* a security patch became available, and implementing the patch does *not* remove their unauthorized access.

3) **Many organizations have performed incomplete investigations and may remain compromised by sophisticated threat actors.**
Why? Initial reports misclassified the threat, leading investigators to only search for dangerous files (i.e., webshells). Onapsis was able to reconstruct the real zero-day attacks, which improved investigative techniques needed to detect stealth attacks.

Actions to Take Today

The following actions are strongly recommended to protect your organization:

1) Have your teams apply the cumulative SAP Security Note 3604119 immediately
2) If patching is not possible, implement the recommended workaround from SAP and/or restrict network access if possible.
3) Perform an in-depth compromise assessment of potentially-impacted systems.
4) Implement SAP-endorsed, dedicated SAP application cybersecurity controls.

Detailed technical information and additional resources can be found here.

Contact Onapsis Experts for SAP Incident Response or Additional Guidance at

rapidresponse@onapsis.com