- Risk Management
- Compliance
- Privacy
- Supply Chain

- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - Network Security
  - Application Security
- Security Strategy
  - Risk Management
  - Security Architecture
  - Disaster Recovery
  - Training & Certification
  - Incident Response
- ICS/OT
- IoT Security

Home › Vulnerabilities

Critical SAP Vulnerability Allows Supply Chain Attacks

By Ionut Arghire on January 17, 2022

A critical vulnerability addressed recently in SAP NetWeaver AS ABAP and ABAP Platform could be abused to set up supply chain attacks, SAP security solutions provider SecurityBridge warns.

Tracked as CVE-2021-38178 and featuring a CVSS score of 9.1, the critical vulnerability was addressed on the October 2021 SAP Patch Day.

Described as an improper authorization issue, the security error allows an attacker to tamper with transport requests, thus bypassing quality gates and transferring code artifacts to production systems.

Production systems are typically at the end of the line in SAP instances for development, integration, and testing, with all instances often sharing a central transport directory, where files needed for deploying changes from development to production are stored.

Transport requests are used to deploy modifications throughout the SAP system line, and these requests are assumed to be unmodifiable once exported. Thus, for any new change, a different request would be needed.

However, SecurityBridge discovered that standard SAP deployments include a program that does allow employees with specific authorization levels to change the header attributes of SAP transport requests.

Because of that, an attacker or a malicious insider with sufficient permissions on a compromised system has a window of opportunity between the export of transport requests and their import into production units, when they could change the release status from ”Released” to ”Modifiable.”

A transport request can be tampered with after it has passed all quality gates, and the attacker could add a payload to be executed after import into a target system, thus opening the door to supply chain attacks.

“Attackers may introduce malicious code into the SAP development stage, unseen, even into requests that have already been imported into the test stage. They could alter the transport request content just before promotion into production, allowing for code execution,” SecurityBridge notes.

All SAP environments where a single transport directory is used at various staging levels are vulnerable and organizations are advised to apply the available patches and check for manipulations of transport requests before importing into production.

Related: SAP Patches Log4Shell Vulnerability in More Applications

Related: SAP Patches Log4Shell Vulnerability in 20 Applications

Related: SAP Patches Critical Vulnerability in ABAP Platform Kernel

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

Additional Healthcare Firms Disclose Impact From Netgain Ransomware Attack
Vulnerability in IDEMIA Biometric Readers Allows Hackers to Unlock Doors
Safari 15 Vulnerability Allows Cross-Site Tracking of Users
Critical SAP Vulnerability Allows Supply Chain Attacks
Details Published on AWS Flaws Leading to Data Leaks

Tags:

NEWS & INDUSTRY Vulnerabilities