SecureArc
Security Solutions *for SAP® software*

Automatically identify security weaknesses and corresponding remediation actions for your SAP® systems

HIGHLIGHTS

- SecureArc's Security Solutions *for SAP® software* offer an efficient method to verify the security posture of your SAP® systems
- It is a non-invasive SAP® security assessment solution using security data extracted from your SAP® systems
- Consists of SecureArc's Security Analyzer *for SAP® software* and SecureArc's Code Analyzer *for SAP® software*

SecureArc's Security Solutions for SAP® are designed to give you a quick overview on the security posture of your SAP® systems based on the ABAP stack and provides you with the opportunity to analyze custom ABAP code on the fly.

SAP® SYSTEM COVERAGE

SecureArc's Security Solutions *for SAP® software* are designed to analyze the security posture of every SAP® application based on the ABAP stack.

SECURITY ANALYZER *for SAP® software* – YOUR VALUE

This module delivers you reports containing security relevant Information about your SAP® system. Test results as wells as measures to optimize the security of your system(s) are automatically generated and presented in lucid reports.

CODE ANALYZER *for SAP® software* – YOUR VALUE

This module delivers you a report regarding security weaknesses for any desired ABAP code. The Code Analyzer performs a fully automated check on the ABAP code and generates a report with identified weaknesses and associated measures.

HOW TO GET IT

Get in contact with us via contact@securearc.ch to either get a software license or to subscribe for a managed service.

Test ID	Test	Count	Risk Score
SEC.01-00	SAP Gateway Security Configuration (secinfo)	5	No risk
SEC.01-01	SAP Message Server Configuration	8	Critical
SEC.01-02	SAProuter Permission Table	24	No risk
SEC.01-03	SAP Gateway Security Configuration (reginfo)		
SEC.01-04	Security Audit Log		

Report SEC.01-01   **Critical**

Test Description
This report shows the content of the message server access control list as specified in the system profile parameter "ms/acl_info". The message server represents the central communication component in an SAP system network and should therefore be protecte

Recommendation
Maintain the Message Server ACL file in order to restrict the access of application servers, which are allowed to log on to the message server of this system. Refer to SAP Note "821875" for further implementation details.

Get Selection Criteria   **Export To Excel**

CONTENT
Search CON
This file controls which hosts can connect to the message server
Syntax:
HOST=[* | ip_adr | host_name | Subnet_mask | Domain] [, ...]
#
# Examples for valid entries are:
# HOST=* (all hosts are allowed)
# HOST=host1,host2 (host1 and host2 can log on)
HOST=*

www.securearc.ch