

SAP Netweaver IUUC_RECON_RC_COUNT_TABLE_BIG ABAP Code Injection

Authored by [Raschin Tavakoli](#) | Site [sec-consult.com](#)

Posted Dec 15, 2021

SAP Netweaver version SAP DMIS 2011_1_731 SP 0013 suffers from a remote ABAP code injection vulnerability in IUUC_RECON_RC_COUNT_TABLE_BIG.

tags | [exploit](#), [remote](#)

advisories | [CVE-2021-33701](#)

SHA-256 | [faf208cedd4dc5530fc5003cbe8bb903e10dfc267c17f5c9a76ed71c5665aa617](#) [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

[Change Mirror](#)[Download](#)

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 ADRC 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'])
```

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu11security 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (6,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older
File Inclusion (4,165)	

Systems

File Upload (946)	
Firewall (821)	AIX (426)
Info Disclosure (2,660)	Apple (1,926)
Intrusion Detection (867)	BSD (370)
Java (2,899)	CentOS (55)
JavaScript (821)	Cisco (1,917)
Kernel (6,291)	Debian (6,634)
Local (14,201)	Fedora (1,600)
Magazine (586)	FreeBSD (1,242)
Overflow (12,419)	Gentoo (4,272)
Perl (1,418)	HPUX (878)
PHP (5,093)	iOS (330)
Proof of Concept (2,291)	iPhone (108)
Protocol (3,435)	IRIX (220)
Python (1,467)	Juniper (67)
Remote (30,044)	Linux (44,315)
Root (3,504)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,777)	OpenBSD (479)
Shell (3,103)	RedHat (12,469)
Shellcode (1,204)	Slackware (941)
Sniffer (886)	Solaris (1,607)

```
[ --- 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
```

Spoof (2,166)	SUSE (1,444)
SQL Injection (16,102)	Ubuntu (8,199)
TCP (2,379)	UNIX (9,159)
Trojan (686)	UnixWare (185)
UDP (676)	Windows (6,511)
Virus (662)	Other
Vulnerability (31,136)	
Web (9,365)	
Whitepaper (3,729)	
x86 (946)	
XSS (17,494)	
Other	

[Login](#) or [Register](#) to add favorites

packet storm

© 2022 Packet Storm. All rights reserved.

Site Links

[News by Month](#)

[News Tags](#)

[Files by Month](#)

[File Tags](#)

[File Directory](#)

About Us

[History & Purpose](#)

[Contact Information](#)

[Terms of Service](#)

[Privacy Statement](#)

[Copyright Information](#)

Hosting By

[Rokasec](#)



Follow us on Twitter



Subscribe to an RSS Feed