

Search .

Home Files News About Contact &[SERVICES_TAB]

Add New

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

adysories | CVE-2021-33701
SHA-256| faf208cedd4dc5530fc5003cbe8bb903e10df267c17f5c9a76ed71c5665aa617
Download | Favorite | View

Related Files

Share This

Like

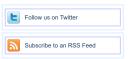
TWO

LinkedIn

Reddit Digg

StumbleUpon







Тор	Authors In Last 30 Days
Red H	at 157 files
Ubunt	u 76 files
Liquid	IWorm 23 files
Debia	n 21 files
nu11s	ecur1ty 11 files
malvu	In 11 files
Gento	O 9 files
Googl	e Security Research 8 files
Julien	Ahrens 4 files
T. Wel	per 4 files

File Tags File Archives December 2022 Advisory (79,754) Arbitrary (15.694) October 2022 RRS (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) File Upload (946) Systems 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 (1,690) 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) Mac OS X (684) Ruby (594) Mandriva (3.105) Scanner (1.631) 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")
            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|ENDEVELOPER |
001|EST |
001|E_TEST |
001|E_TEST |
001|DIC |
001|SAP* |
  Sending payload ...
USREFUS after:
001|BMDEVELOPER |
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.
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-21-0019 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 CVW-2021-37301 (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
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 workscound.
 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.
  https://sec-consult.com/vulnerability-lab/
 SEC Consult Vulnerability Lab
About SEC Consult Vulnerability Lab
The SEC Consult Vulnerability Lab is an integrated part of SEC Consult, an Akos 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 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 / 02021
```

Login or Register to add favorites

File Directory

packet storm © 2022 Packet Storm. All rights reserved.

Site Links About Us News by Month History & Purpose News Tags Contact Information Files by Month File Tags

Terms of Service Privacy Statement Copyright Information **Hosting By** Rokasec





SUSE (1,444)

UNIX (9 159)

UnixWare (185)

Windows (6,511)

Other

SQL Injection (16,102) Ubuntu (8,199)

Spoof (2,166)

TCP (2.379)

UDP (876)

Virus (662)

x86 (946)

XSS (17,494) Other

Vulnerability (31,136) Web (9,365) Whitepaper (3,729)