iTech Workshop®

Data Integration for Healthcare

expEDIum Medical Billing

v4.1.0

Release Notes

Release Date | Oct 24, 2018

Table of Contents

Release Notes

1) [Ticket# 3591] Error:14 - Box:28 - Validation failing

The validation error reported on Box 18 (*Error Code: 14 | Error Description: Balance Validation Failed*) sporadically on some claims during traffic conditions when claims in bulk are processed. This was due to a database commit issue, which we rectified and fixed. The hot patch is applied on Sep 08, 2018 as v4.0.1.1 on servers running on WildFly.

2) [Ticket# 7554, 7911] Application Security Tightening

As part of the tightening the application security, we have enhanced the web module in the product to have various security measures in handling the page requests. The security measures are implemented to handle the following -

1. **XSS (Cross Site Scripting)**

   Using the library "JSoup", all the request parameters are filtered and all script and html tags passed in the request are removed if found. There are exceptions where the application itself passes HTML snippets in a couple of feature. This request is relaxed to allow the HTML tag.

2. **Arbitrary File Download**

   This security measure is applied on all the file download links in the product and will ensure only the respective file is downloaded all the time.

3. **Unrestricted File Upload**

   As a security measure, we have introduced restrictions on files that can be uploaded to various file upload screens. The restrictions are based on the extension of the files.
   The while list of the file extensions is configured in the application properties file "eCP.properties".
   These are the allowed file extensions and various module where it is implemented –

   1) **upload.image.allowed.extensions= gif,ico,png,jpeg,jpg**

This whitelisting is applied on Administrator Account Logo Upload Screen under Administrator Login, Patient Attachment Screen and Claim Attachment Screen.

2) **upload.payload.allowed.extensions=txt,hcfa,nsf,csv,xml,json,hl7,837p,837i,837,clm, edi,x12n,x12,zip**
   This whitelisting is applied on Send Batch Screen, and Patient Import Screen.

3) **upload.payer.reports.allowed.extensions=txt,edi,x12n,x12,835,era,ebt,ta1,html,htm, 271,997,999,277,277ca,824,864,zip**
   This whitelisting is applied on ERA Upload Screen under Administrator Login.

4) **upload.template.allowed.extensions=html,htm**
   This whitelisting is applied on Ledger Receipt Template Upload Screen and Debt Set Off Letter Temple Upload Screen under Administrator Login.

5) **upload.map.allowed.extensions=txt,props,properties,csv,xml**
   This whitelisting is applied on Claim Print Map Upload Screen and Fee Schedule Map Upload Screen under Administrator Login

6) **upload.document.allowed.extensions=txt,pdf,xls,xlsx,doc,docx,rtf,odt**
   This whitelisting is applied on Patient Attachment Screen and Claim Attachment Screen.

Also, the maximum size of the file that can be uploaded from all the screens is configurable from the application configuration file as shown below (it was not configurable earlier). The default file size is 50MB. This would mean any of the files uploaded (such as Claim batch EDI or CSV or XML files, patient & claim attachments. This is also applicable to the size of reports that are exported as CSV, PDF and Excel.)

allowed.max.size.for.file.upload=52428800

This is same as that of the maximum size of the http request content configured in the application server http listener configuration.

4. CSRF (Cross Site Request Forgery)

A 32-character random UUID is generated for each session and this is passed in all the requests in the application. Before the request is processed, we ensure that this UUID in the request is same as that the UUID stored in session when the session was created. If this UUID is different, or if the UUID is not present in the request, the session will be invalidated and the user will be redirected to a page which displays "Unauthorized Request. Please contact the administrator". All the page requests in the production are changed to accommodate this new variable "requestID".

5. Browser Cache Management

We have ensured that the pages are filtered using cache prevention logic to tell browser not to cache.

Filter Code:

```
httpresponse.setHeader("Cache-Control", "no-cache, no-store, must-revalidate");
httpresponse.setHeader("Pragma", "no-cache");
httpresponse.setDateHeader("Expires", 0);
httpresponse.setHeader("session.cache_limiter","public");
```

6. Clickjacking

This requires blocking expEDIum access over iFrames. expEDIum should allow other applications to seamlessly integrate using Web APIs over iFrames, this security measure is relaxed.

7. **Password Policy – Change Password**

   The logic of comparing "new password" and "confirm password" is completely moved to server side from client side as part of tightening the security.

3) [Ticket# 8565] Fix for Patient Statement Logo Not Found error

The application server logs were having File Not Found exception on patient statement header logo for all patient statements, even though the statement header is configured as text. Note, the statement is successfully getting created even with this exception reported in logs. The logic in the patient statement module is enhanced by adding additional preconditions, as a fix to this issue.

This fix is applied as a hot patch (v3.6.8.4011) on Sep 05, 2018 one of the application servers running on JBoss Platform. All the other servers running on WildFly Platform is upgraded to have this hot patch (v4.0.1.1) on Sep 08, 2018. The JBoss version of the product (used as Plan B) on all the WildFly powered servers were also upgraded to v3.6.8.4011 on Sep 08, 2018.

4) [Ticket# 8574] PH: XML Payload Parsing Issue

One of the servers while running on the new technology platform of WildFly experienced intermittent issues in parsing claim XML payloads when processed in bulk on high traffic conditions. This was due to glitch in WildFly migration. The server was reverted to the previous platform JBoss, for a smooth functioning. The issue was reproduced locally under high load conditions, fixed and a hot patch is deployed on Sep 08, 2018. The application is also switched to WildFly platform after the patch is applied.

5) [Ticket# 8597] iTech: Input Prof Claim CSV | Fix for Diagnosis Code Pointers

While processing claims in CSV format the diagnosis code pointers populated as "1,2,3" (with double quotes to handle embedded commas) is converted to ,1,2,3, by expEDIum. This issue is not happening when there is only one pointer in the service line and that is populated without double quotes.

There was a glitch in the code to format diagnosis code which is fixed and deployed as a hot patch on the production and demo servers as v4.0.1.2 on Sep 17, 2018.

6) [Ticket# 8618] WildFly | Process Scheduler Issue | Creating 2 tasks for each trigger

It was observed that the automated triggers are creating two tasks in one trigger. Few Java annotations related to scheduler and EJBs were wrongly specified during the migration of code. This is fixed and a hot patch was released on all production and demo servers as v4.0.1.2 on Sep 17, 2018.

7) [Ticket# 8720] XSS - Escape Character Handling

While handling the security tightening on XSS, it was noticed that the characters **&, <, > and '** were converted to **& > < and &quot**; respectively by the JSoup Library used. These characters when present in password fields were causing validation issues during login.

All the special characters are "unescaped" (to avoid the conversion) using an API method available in the library to handle this issue. This patch was labelled as v4.1.0.1

There was also a session expiry issue when user logout and logs in again from Internet Explorer 11, Edge when http/2 is turned ON and on all browsers when http/2 is false. This is fixed and labelled as v4.1.0.2 – this is official release of v4.1.0.

We noticed during the final stages of testing that character "<" still has an issue when used in the passwords and hence request you NOT to use "<" character in passwords. We have taken the liberty to change a few passwords that had "<" embedded, not to have that character. We are working on fixing this and the fix shall be available in the next immediate release.

Bugzilla List of tickets available in this release

#	iTech Ticket#	Client	Client Ticket #	Summary	Version
1	3591			Error:14 - Box:28 - Validation failing	v4.0.1.1
2	7544, 7911			Application Security Tightening	V4.1.0
3	8565	Patagonia		Fix for Patient Statement Logo Not Found error	v3.6.8.4011, v4.0.1.1
4	8574	Patagonia		PH: XML Payload Parsing Issue	V4.01.1
5	8597			iTech: Input Prof Claim CSV | Fix for Diagnosis Code Pointers	V4.0.1.2
6	8618			WildFly | Process Scheduler Issue | Creating 2 tasks for each trigger	V4.0.1.2
7	8720			XSS - Escape Character Handling	V4.1.0.1

***** END OF DOCUMENT *****