Base Language - Bug #3251

implement safe and secure processing of procedure manager parameters when up-called from javascript

02/22/2017 08:02 AM - Greg Shah

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
billable:	No	**case_num:**	
vendor_id:	GCD	**version:**	

Description

History

#1 - 02/22/2017 08:03 AM - Greg Shah

From #3209-731:

I mistakenly passed a javascript Date object instead of a string to the loadRooms function in ehotel.js and I got this:

```
Caused by: java.lang.NullPointerException
        at java.util.ArrayDeque.addFirst(ArrayDeque.java:228)
        at java.util.ArrayDeque.push(ArrayDeque.java:503)
        at com.goldencode.p2j.util.ProcedureManager$CalleeInfoImpl.push(ProcedureManager.java:2882)
        at com.goldencode.p2j.util.ProcedureManager$WorkArea.scopeStart(ProcedureManager.java:2484)
        at com.goldencode.p2j.util.TransactionManager.processScopeNotifications(TransactionManager.java:5274)
        at com.goldencode.p2j.util.TransactionManager.pushScope(TransactionManager.java:1858)
        at com.goldencode.p2j.util.BlockManager.topLevelBlock(BlockManager.java:6700)
        at com.goldencode.p2j.util.BlockManager.internalProcedure(BlockManager.java:321)
        at com.goldencode.p2j.util.BlockManager.internalProcedure(BlockManager.java:307)
        at com.goldencode.hotel.Ehotel.inMsgLoadRooms(Ehotel.java:1159)
        at sun.reflect.GeneratedMethodAccessor868.invoke(Unknown Source)
        at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
        at java.lang.reflect.Method.invoke(Method.java:497)
        at com.goldencode.p2j.util.ControlFlowOps$InternalEntryCaller.invokeImpl(ControlFlowOps.java:5335)
        at com.goldencode.p2j.util.ControlFlowOps$InternalEntryCaller.invoke(ControlFlowOps.java:5313)
        at com.goldencode.p2j.util.ControlFlowOps.invokeImpl(ControlFlowOps.java:4374)
        at com.goldencode.p2j.util.ControlFlowOps.invoke(ControlFlowOps.java:3225)
        at com.goldencode.p2j.ui.LogicalTerminal.lambda$invoke$117(LogicalTerminal.java:14455)
        at com.goldencode.p2j.ui.LogicalTerminal$$Lambda$85/187125032.get(Unknown Source)
        at com.goldencode.p2j.ui.LogicalTerminal.invokeOnServer(LogicalTerminal.java:14977)
        at com.goldencode.p2j.ui.LogicalTerminal.invoke(LogicalTerminal.java:14455)
        at sun.reflect.GeneratedMethodAccessor428.invoke(Unknown Source)
        at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
        at java.lang.reflect.Method.invoke(Method.java:497)
        at com.goldencode.p2j.util.MethodInvoker.invoke(MethodInvoker.java:76)
        at com.goldencode.p2j.net.Dispatcher.processInbound(Dispatcher.java:709)
        at com.goldencode.p2j.net.Conversation.block(Conversation.java:364)
        at com.goldencode.p2j.net.Conversation.waitMessage(Conversation.java:300)
        at com.goldencode.p2j.net.Queue.transactImpl(Queue.java:1128)
        at com.goldencode.p2j.net.Queue.transact(Queue.java:599)
        at com.goldencode.p2j.net.BaseSession.transact(BaseSession.java:223)
        at com.goldencode.p2j.net.HighLevelObject.transact(HighLevelObject.java:163)
        at com.goldencode.p2j.net.RemoteObject$RemoteAccess.invokeCore(RemoteObject.java:1425)
        at com.goldencode.p2j.net.InvocationStub.invoke(InvocationStub.java:97)
        at com.sun.proxy.$Proxy16.waitFor(Unknown Source)
        at com.goldencode.p2j.ui.LogicalTerminal.waitFor(LogicalTerminal.java:6278)
        at com.goldencode.p2j.ui.LogicalTerminal.waitFor(LogicalTerminal.java:6048)
        at com.goldencode.hotel.Emain.lambda$execute$84(Emain.java:1013)
        at com.goldencode.hotel.Emain$$Lambda$59/179123375.body(Unknown Source)
        at com.goldencode.p2j.util.Block.body(Block.java:556)
        at com.goldencode.p2j.util.BlockManager.processBody(BlockManager.java:6937)
```

```
        at com.goldencode.p2j.util.BlockManager.topLevelBlock(BlockManager.java:6728)
        at com.goldencode.p2j.util.BlockManager.externalProcedure(BlockManager.java:295)
        at com.goldencode.p2j.util.BlockManager.externalProcedure(BlockManager.java:269)
        at com.goldencode.hotel.Emain.execute(Emain.java:453)
        at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
        at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62)
        at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
        at java.lang.reflect.Method.invoke(Method.java:497)
        at com.goldencode.p2j.util.Utils.invoke(Utils.java:1288)
        at com.goldencode.p2j.main.StandardServer$MainInvoker.execute(StandardServer.java:1827)
        at com.goldencode.p2j.main.StandardServer.invoke(StandardServer.java:1322)
        at com.goldencode.p2j.main.StandardServer.standardEntry(StandardServer.java:461)
        at sun.reflect.GeneratedMethodAccessor674.invoke(Unknown Source)
        at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
        at java.lang.reflect.Method.invoke(Method.java:497)
        at com.goldencode.p2j.util.MethodInvoker.invoke(MethodInvoker.java:76)
        at com.goldencode.p2j.net.Dispatcher.processInbound(Dispatcher.java:709)
        at com.goldencode.p2j.net.Conversation.block(Conversation.java:364)
        at com.goldencode.p2j.net.Conversation.run(Conversation.java:184)
        at java.lang.Thread.run(Thread.java:745)
```

The same error occurred when I passed a date string in the wrong format.

This is not high priority, but we will need to handle invalid parameters in upcalls more gracefully than tripping on an NPE, since it is pretty easy to pass garbage in from javascript.