# Core Development - Bug #2932

## Apache Commons Collections Java Library Vulnerability

12/12/2015 11:01 AM - Sergey Ivanovskiy

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | 12/12/2015 |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | Sergey Ivanovskiy | **% Done:** | 100% |
| **Category:** | | **Estimated time:** | 0.00 hour |
| **Target version:** | GUI Support for a Complex ADM2 App | | |
| **billable:** | No | **case_num:** | |
| **vendor_id:** | GCD | | |

**Description**

### History

**#1 - 12/12/2015 11:02 AM - Sergey Ivanovskiy**

The task history is listed below.
On 12/09/2015 11:20 AM, Eric Faulhaber wrote:

> These are easily replaced with:
>
> Collections.unmodifiableList
> List.isEmpty
>
> respectively, from the java.util package.
>
> Thanks,
> Eric
>
> On 12/09/2015 11:10 AM, Serg Ivanovskiy wrote:
>
> > Greg, Eric
> >
> > Ok, understand. The direct usages from p2j code are below
> > CollectionUtils.unmodifiableCollection() by FieldGroup.java
> > CollectionUtils.isEmpty() by ThinClient.java
> >
> > found using "import org.apache.commons.collections.*" package
> >
> > Sergey
> >
> > On 12/09/2015 06:48 PM, Greg Shah wrote:
> >
> > > Sergey,
> > >
> > > I'm wanting to know if we use classes from apache collections directly from P2J code.
> > >
> > > Thanks,
> > > Greg
> > >
> > > On 12/09/2015 10:35 AM, Serg Ivanovskiy wrote:
> > >
> > > > Greg,
> > > >
> > > > Found that this revision added lib/commons-collections-3.2.1.jar.
> > > >
> > > > revno: 10496
> > > > committer: Constantin Asofiei <ca@goldencode.com>
> > > > branch nick: p2j
> > > > timestamp: Wed 2014-03-26 07:32:09 -0400
> > > > message:
> > > > Implemented graph DB-based callgraph processing (backed by Titan DB). Refs #2251
> > > >
> > > > Sergey.

On 12/09/2015 06:08 PM, Greg Shah wrote:

> Sergey,
>
> Yes, I have seen this too.  This is one of many reasons that we try to limit the use of 3rd party libraries.
>
> Nobody at GCD is supposed to be using the apache collections in P2J.  However, I have seen some usage from time to time.  When I've seen this usage in the past I've asked for it to be removed, but I doubt I have found all cases. Would you please do a search on the trunk to see where these may have (inappropriately) been added?
>
> Thanks,
> Greg
>
> On 12/09/2015 09:24 AM, Serg Ivanovskiy wrote:
>
> > Greg,
> >
> > Yesterday, I have found this original report about deserialization vulnerability in java applications if they use Apache Commons Collection library, InvokerTransformer class is recommended to remove from commons-collections-*.jar.
> > http://foxglovesecurity.com/2015/11/06/what-do-weblogic-websphere-jboss-jenkins-opennms-and-your-application-have-in-common-this-vulnerability/
> >
> > The official reports are here:
> > https://www.us-cert.gov/ncas/current-activity/2015/11/13/Apache-Commons-Collections-Java-Library-Vulnerability
> > http://www.kb.cert.org/vuls/id/576313
> >
> > Seregy

**#2 - 12/12/2015 11:08 AM - Sergey Ivanovskiy**

Official fixes: http://commons.apache.org/proper/commons-collections/release_4_1.html,

http://commons.apache.org/proper/commons-collections/release_3_2_2.html

#### #3 - 12/12/2015 12:56 PM - Sergey Ivanovskiy

*- File commons-collections-3.2.2.diff.txt added*

Greg, please review this diff, the new version http://commons.apache.org/proper/commons-collections/release_3_2_2.html has some fix for the serialization vulnerability.

#### #4 - 12/12/2015 03:30 PM - Greg Shah

Code Review commons-collections-3.2.2.diff.txt

The changes are fine.  Please commit them to 1811t.  I guess you should include the newer 3.2.2 version as long as Hibernate is compatible.

#### #5 - 12/13/2015 11:46 AM - Sergey Ivanovskiy

Committed revision 10962. Release notes for 3.2.2 claims that it is compatible with 3.2 and it is only bug fixes for 3.2.1, thus it should be compatible with the current hibernate version. It seems that it doesn't add new bugs to customer's 454 testcase. Greg, please check commons-collections-3.2.2.jar with the official one in order to be sure that it is original. I did this check based on the provided official md5 sum https://commons.apache.org/proper/commons-collections/download_collections.cgi for its binary distribution zip file, because all my java faults were due to the hardware memory faults and yesterday it was clear for me.

#### #6 - 12/17/2015 08:14 AM - Greg Shah

*- Status changed from New to Closed*

*- Target version set to Milestone 12*

*- % Done changed from 0 to 100*

Yes, I have confirmed this is the official binary.

#### #7 - 11/16/2016 12:12 PM - Greg Shah

*- Target version changed from Milestone 12 to GUI Support for a Complex ADM2 App*

### Files

| | | | |
|---|---|---|---|
| commons-collections-3.2.2.diff.txt | 1.83 KB | 12/12/2015 | Sergey Ivanovskiy |