

Java Debug Port

Meetup 15.02.2017 - Sergej

Java Platform Debugger Architecture (JPDA)

- ✦ Java Virtual Machine Tool Interface (JVM TI)
- ✦ Java Virtual Machine Debug Interface (JVMDI)
- ✦ Java Debug Wire Protocol (JDWP)
- ✦ Java Debug Wire Protocol Interface
- ✦ Java Debug Interface (JDI)

Beispiel Tomcat

- ✦ Der Default Debug Port ist 8000
- ✦ Tomcat Konfiguration

```
export JPDA_ADDRESS=8000
export JPDA_TRANSPORT=dt_socket
bin/catalina.sh jpda start
```

- ✦ Default-Binding ist 0.0.0.0

```
user@linux:~$ netstat -tulpn | grep -i "8000"
Proto Local Address Foreign Address State      PID/Program name
tcp    0.0.0.0:8000  0.0.0.0:*      LISTEN    2751/java
```


Sicherheitsprobleme

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3292>



Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

[Search CVE List](#) | [Download CVE](#) | [Update an ID](#) | [Request a CVE ID](#)

[Home](#) | [CVE IDs](#) | [About CVE](#) | [Compatible Products & More](#) | [Community](#) | [Blog](#) | [News](#) | [Site Search](#)

TOTAL CVE IDs: 81598

[HOME](#) > [CVE](#) > [CVE-2015-3292](#)

Section Menu

CVE IDs

[Updates & Feeds](#)

Request a CVE ID

[Contact a CVE Numbering Authority \(CNA\)](#)

[Contact Primary CNA \(MITRE\) – CVE Request web form](#)

[Reservation Guidelines](#)

CVE LIST (all existing CVE IDs)

[Downloads](#)

[Search CVE List](#)

[Search Tips](#)

[Printer-Friendly View](#)

CVE-ID

CVE-2015-3292

[Learn more at National Vulnerability Database \(NVD\)](#)


• [Severity Rating](#) • [Fix Information](#) • [Vulnerable Software Versions](#) • [SCAP Mappings](#)

Description


The installer in NetApp OnCommand Workflow Automation before 2.2.1P1 and 3.x before 3.0P1 sets up the Java Debugging Wire Protocol (JDWP) service, which allows remote attackers to execute arbitrary code via unspecified vectors.

Sicherheitsprobleme

[https://nvd.nist.gov/cvss/v2-calculator?name=CVE-2015-3292&vector=\(AV:N/AC:L/Au:N/C:C/I:C/A:C\)](https://nvd.nist.gov/cvss/v2-calculator?name=CVE-2015-3292&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C))



Sponsored by
DHS/NCCIC/US-CERT



NIST
National Institute of
Standards and Technol

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities	Checklists	800-53/800-53A	Product Dictionary	Impact Metrics	Data Feeds	Statistics	FAQs
Home	SCAP	SCAP Validated Tools	SCAP Events	About	Contact	Vendor Comments	Visualizations

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

- 82543 [CVE Vulnerabilities](#)
- 427 [Checklists](#)
- 249 [US-CERT Alerts](#)
- 4460 [US-CERT Vuln Notes](#)
- 10286 [OVAL Queries](#)
- 117168 [CPE Names](#)

Last updated: 2/14/2017 4:23:59 PM

CVE Publication rate: 31.93

Email List

Common Vulnerability Scoring System Version 2 Calculator - CVE-2015-3292

This page shows the components of the [CVSS](#) score for example and allows you to refine the CVSS base score. Please read the [CVSS standards guide](#) to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

Base Scores



Category	Score
Base	10.0
Impact	10.0
Exploitability	10.0

Sicherheitsprobleme

<https://www.exploit-db.com/exploits/33789/>



Java - Debug Wire Protocol Remote Code Execution (Metasploit)

EDB-ID: 33789	Author: Metasploit	Published: 2014-06-17
CVE: CVE-2015-3292	Type: Remote	Platform: Multiple
Aliases: N/A	Advisory/Source: N/A	Tags: Metasploit Framework
E-DB Verified:	Exploit: Download / View Raw	Vulnerable App: N/A

```
71 def initialize
72   super(
73     'Name'          => 'Java Debug Wire Protocol Remote Code Execution',
74     'Description'    => %q{
75       This module abuses exposed Java Debug Wire Protocol services in order
76       to execute arbitrary Java code remotely. It just abuses the protocol
77       features, since no authentication is required if the service is enabled.
78     },
79     'Author'         => [
80       'Michael Schierl', # Vulnerability discovery / First exploit seen / Msf
81       'Christophe Alladoux', # JDWP Analysis and Exploit
82       'Redsadic <julian.vilas[at]gmail.com>' # Metasploit Module
83     ],
84     'References'     =>
```


Demo

Gegenmaßnahmen

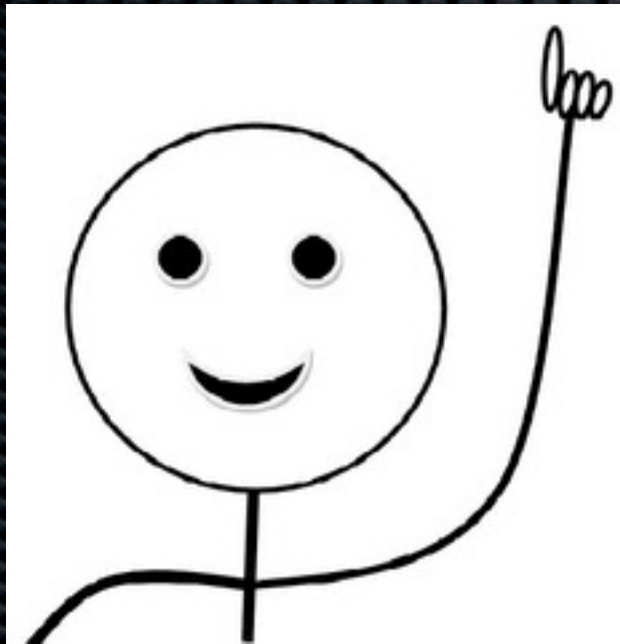
- ✦ Java Debug Ports mit Localhost-Binding starten
- ✦ Beispiel Tomcat

```
export JPDA_ADDRESS=127.0.0.1:8000
export JPDA_TRANSPORT=dt_socket
bin/catalina.sh jpda start
```

- ✦ Beispiel Localhost-Binding

```
user@linux:~$ netstat -tulpn | grep -i "8000"
Proto Local Address  Foreign Address  State  PID/Program name
tcp    127.0.0.1:8000  0.0.0.0:*        LISTEN 2751/java
```


Fragen?



Quellen

<https://docs.oracle.com/javase/7/docs/technotes/guides/jpda/>

<https://docs.oracle.com/javase/1.5.0/docs/guide/jpda/jdwp-spec.html>

https://www.rapid7.com/db/modules/exploit/multi/misc/java_jdwp_debugger/

<https://www.exploit-db.com/exploits/33789/>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3292>