



## CVE-2016-0603 – Oracle Issues out-of-box Java emergency patch for Windows

February 8, 2016 By [Pierluigi Paganini](#)



Oracle issued an out-of-box emergency patch for Java platform running on Windows machines that fixes the critical vulnerability coded as CVE-2016-0603.

Oracle issued an out-of-box emergency patch for Java software running on Windows systems that fixes a critical vulnerability coded as **CVE-2016-0603**. The vulnerability could be exploited by an attacker to trick users into visiting a malicious website and downloading files on the target system before installing Java 6, 7 or 8.

Oracle hasn't provided much information on the vulnerability, the flaw has received a CVSS Base Score of 7.6.

*"Oracle just released [Security Alert CVE-2016-0603](#) to address a vulnerability that can be exploited*

Base Score of 7.6.” states the [security advisory](#) published by Oracle. “To be successfully exploited, this vulnerability requires that an unsuspecting user be tricked into visiting a malicious web site and download files to the user’s system before installing Java 6, 7 or 8. Though considered relatively complex to exploit, this vulnerability may result, if successfully exploited, in a complete compromise of the unsuspecting user’s system.

As explained by Oracle, the successful exploitation of the CVE-2016-0603 flaw could result in **“complete compromise”** of the target machine.

The user is exposed to the attack only during the Java installation phase, for this reason, they have no need to upgrade existing Java installation, but that take care if are managing old version of Java prior to 6u113, 7u97 or 8u73 and are installing them. In this last scenario, they have to download the latest Java releases 6u113, 7u97 or 8u73 or later.

Below the list of affected product releases:

Affected product releases and versions:

Java SE	Patch Availability
JDK and JRE 6 Update 111 on Windows only	Java SE
JDK and JRE 7 Update 95 on Windows only	Java SE
JDK and JRE 8 Update 71, 72 on Windows only	Java SE

*“Because the exposure exists only during the installation process, users need not upgrade existing Java installations to address the vulnerability. However, Java users who have downloaded any old version of Java prior to 6u113, 7u97 or 8u73, should discard these old downloads and replace them with 6u113, 7u97 or 8u73 or later.” continues the post.*

Oracle recommends users to ensure that they are running the most recent version of Java SE and that all older releases of the software have been completely removed. Oracle further advises against downloading Java from sites other than Java.com as these sites may be malicious.

Another suggestion is to download Java software only from the official Java.com website to avoid ugly surprises.

**Pierluigi Paganini**

(Security Affairs – Java CVE-2016-0603 flaw, [hacking](#))

Share it please ...



## 1. Java Expert



## SHARE ON



### Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at [Bit4Id](#), firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security) Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, [he is Certified Ethical Hacker at EC Council in London](#). The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog ["Security Affairs"](#) recently named a Top National Security Resource for US. Pierluigi is a

member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and "Digital Virtual Currency and Bitcoin".

PREVIOUS  
ARTICLE

**T9000 backdoor, a sophisticated malware that spies on Skype users**

NEXT ARTICLE  
**Global and Modern Terrorism/Cyber Terrorism**

1. Core Java



2. Java Programming Training



3. Java Tutorials



4. Programming In Java



5. Java Projects





◦ +Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine".

---



**1. Core Java**



---

**2. Java Programming Training**



---

**3. Java Tutorials**



---

**4. Programming In Java**



---

**5. Java Projects**



---

**6. Codes In Java**



---

**7. Java For Beginners**



---

**8. Java Applications**



Copyright 2015 Security Affairs by Pierluigi Paganini  
All Right Reserved.

[Back to top](#) ^