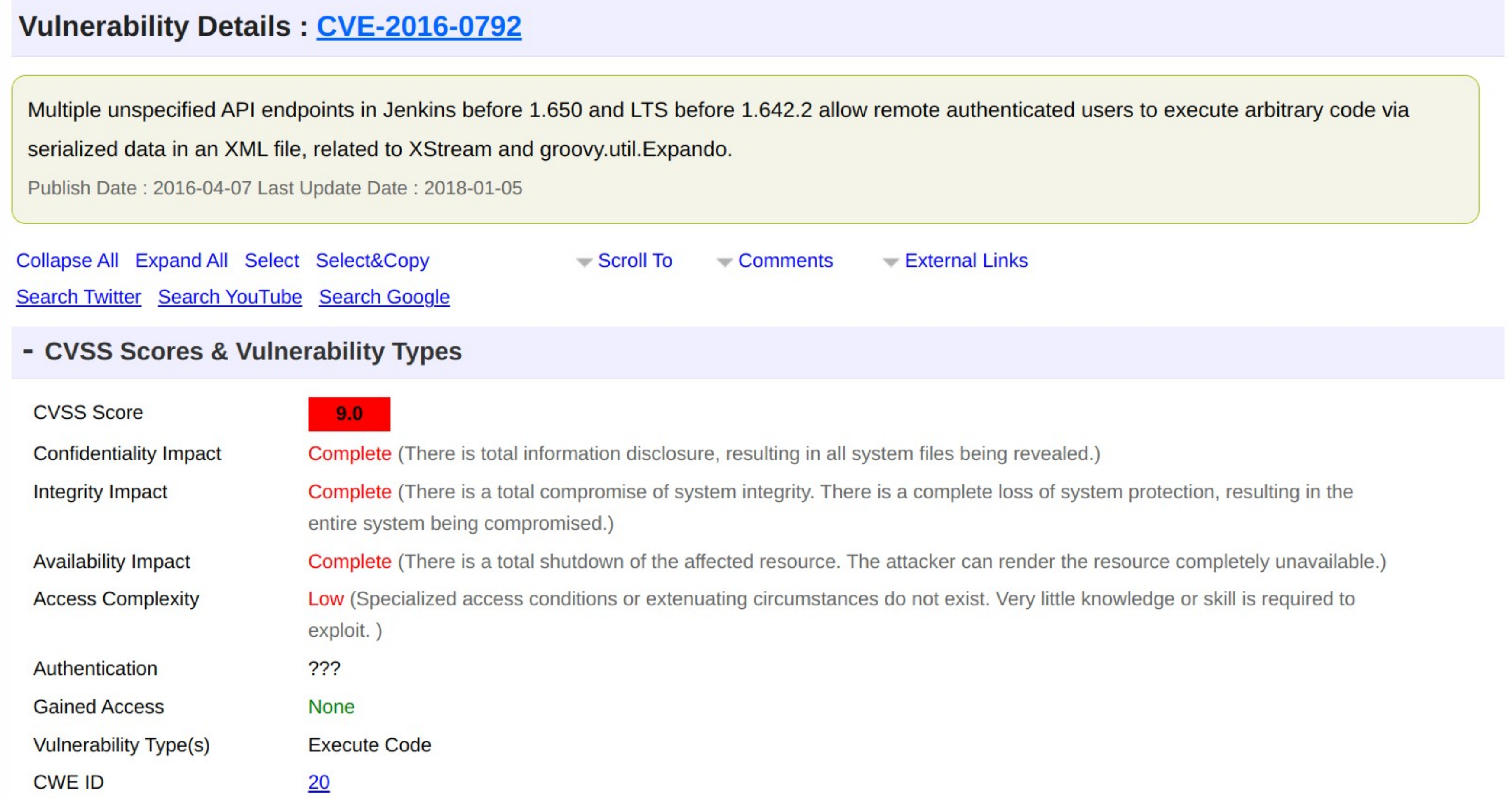
Meethack Torino

Vulnerability Research:
Jenkins - CVE-2016-0792

Jenkins - CVE-2016-0792



Vulnerability Details : CVE-2016-0792

Multiple unspecified API endpoints in Jenkins before 1.650 and LTS before 1.642.2 allow remote authenticated users to execute arbitrary code via serialized data in an XML file, related to XStream and groovy.util.Expando.

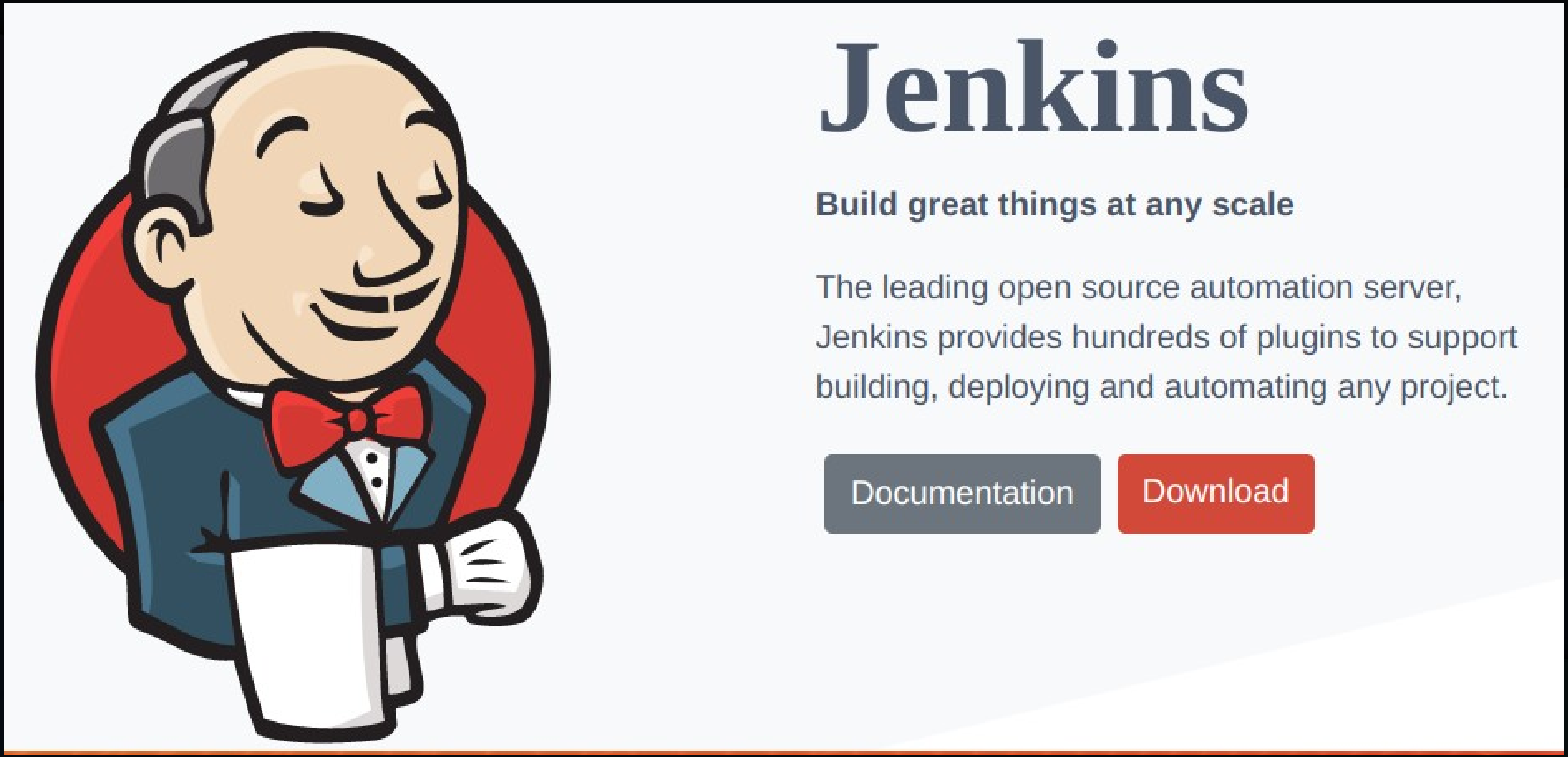
Publish Date : 2016-04-07 Last Update Date : 2018-01-05

- CVSS Scores & Vulnerability Types

CVSS Score	9.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	???
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	20

https://www.cvedetails.com/cve/CVE-2016-0792/

What is Jenkins?



Jenkins

Build great things at any scale

The leading open source automation server, Jenkins provides hundreds of plugins to support building, deploying and automating any project.

https://www.jenkins.io/

Let’s try to “discover” the exploit blindly

- We can use:
  - Bulletin – https://www.jenkins.io/security/advisory/2016-02-24/#remote-code-execution-through-remote-api
  - Vulnerable container – https://hub.docker.com/_/jenkins?tab=tags&page=1&name=1.642.1
  - Vulnerable source code – https://github.com/jenkinsci/jenkins/tree/jenkins-1.642.1
  - Fixed source code – https://github.com/jenkinsci/jenkins/tree/jenkins-1.642.2
- Let’s try not to use:
  - Public exploit – https://github.com/jpiechowka/jenkins-cve-2016-0792
  - Public write-up – https://www.contrastsecurity.com/security-influencers/serialization-must-die-act-2-xstream

Local vulnerable environment

- Setup:

  -
    ```
    docker run -p 1337:8080 -p 50000:50000
    -d --rm --name vuln-jenkins
    jenkins:1.642.1
    ```
  - Connect to `http://localhost:1337`
- Tear down:

  -
    ```
    docker stop vuln-jenkins
    ```