Security Advisory

CSRF Vulnerability detected in JasperServer 3.7.0 CE

1. Background

JasperReports Server is a stand-alone and embeddable reporting server providing robust static and interactive reporting, report server, and data analysis capabilities. These capabilities are available as either standalone products, or as part of an integrated end-to-end BI suite utilizing common metadata and providing shared services, such as security, a repository, and scheduling. JasperReports Server exposes comprehensive public interfaces enabling seamless integration with other applications and the capability to easily add custom functionality (extracted from JasperSoft Wiki Page).

2. Description

During a security test run by CSIRT-cv, we detected that the protection mechanisms against Cross-Site Request Forgery (CSRF) were not enough to prevent malicious actions in the application. One of the parameters (_*flowExecutionKey*) is predictable and can be determined with a very high probability of success in brute-force attacks with less than 100 requests.

As any application, JasperServer has a set of restricted actions that can be performed only by users belonging to the administration role, such as adding or modifying users and roles, changing files and folders permissions, and so on. With social engineering, an attacker can persuade a user belonging to the administration role to click on a malicious link and perform arbitrary actions on the system, if the victim is authenticated into JasperServer.

The structure of the requests JasperServer makes is public, as anyone can download a free version of the program, called Community Edition, and learn how it works. The requests have a parameter that change over time, apparently to control the flow of the application. We discovered that variability and randomization of such parameter is not enough to prevent request forgery attacks, as the parameter can be easily predicted.

To proof this vulnerability, we created a brute force CSRF proof of concept that consisted in a website full of what appeared to be images, each one consisting on a request performing a user addition to JasperServer. When the link is followed by a JasperServer administrator, the user is created.

CVSS Score: 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C). More info about CVSS here.

3. Software affected

The existence of this vulnerability has been tested on JasperServer 3.7.0 Community Edition and JasperServer 3.7.1 Community Edition. Other versions may be affected.

4. Timeline

The timeline of this vulnerability is:

2010/12/15 – Vulnerability confirmed and consistent PoC developed.

2010/12/29 – Vendor contacted.

2011/01/21 – Vendor confirms vulnerability in JasperServer 3.7.0 CE.

2011/01/21 – CERT/CC contacted to manage CVE and disclosure terms with vendor.

2011/04/04 – CERT/CC informs: vendor will release update in late summer.

2011/04/05 – Scheduled publication of advisory to 2011/09/15.

2011/07/19 – CERT/CC informs: vendor reschedules update to the end of october 2011.

2011/07/19 – Release of advisory was already scheduled. No changes will be made.

2011/07/20 – CERT/CC informs: CVE assigned: CVE-2011-1911.

2011/09/07 – Advisory draft sent to CERT/CC for review.

2011/09/15 – Publication of this advisory.

5. Credit

This vulnerability has been discovered and researched by:

- José Vila Montaner from S2Grupo at CSIRT-cv.

With special thanks to the CSIRT-cv team: Guillermo Mir, Maite Moreno, José Miguel Holguín, Alberto Segovia, Manuel Belda, José Luis Chica, Javier Morant and Lourdes Herrero.

6. About CSIRT-cv

CSIRT-cv is the Computer Security Incident Response Team of the Valencian Community, in Spain. It is auspiced by ‘Generalitat de la Comunitat Valenciana’, the Regional Government of the Valencian Community. Its main purpose is to assist members of Valencian Community: citizens, small and medium-sized enterprises and mainly public administration, in implementing proactive measures to reduce the risks of computer security incidents, and also to assist this community in responding to such incidents when they occur.

You can find more information about us on the following sites:

- Web page: http://www.csirtcv.gva.es
- Facebook Profile: http://www.facebook.com/csirtcv
- Twitter Profile: http://www.twitter.com/csirtcv