Alert – JQuery Cross-site Scripting (XSS) vulnerabilities

Description

Cross-Site Scripting (XSS) attacks occur when an attacker tricks a user's browser to execute malicious JavaScript code in the context of a victim's domain. Such scripts can steal the user's session cookies for the domain, scrape or modify its content, and perform or modify actions on the user's behalf, actions typically blocked by the browser's Same Origin Policy.

These attacks are possible by escaping the context of the web application and injecting malicious scripts in an otherwise trusted website.

Impact of the vulnerability

This vulnerability allows remote attackers to inject arbitrary web script or HTML via the close text parameter of the dialog function and it gives an unauthorized control to the website running jQuery and inject malicious files that can redirects the visitor to the malicious links.

Vulnerable versions

- All jQuery versions before 3.3.1 are vulnerable to XSS.
- Affected jQuery package, versions <3.0.0-beta1 >1.12.3 || <1.12.0 >=1.4.0

Solution: Rw-CSIRT is strongly recommending users to:

- Upgrade jQuery java script code to the latest version which is 3.3.1

Affected users should:

Affected users should contact RW-CSIRT: Call; 4045 or write to security@risa.rw to help for analyzing the source of the incident and recommendation.

References:

1. https://snyk.io/vuln/npm:jquery:20150627
2. https://snyk.io/vuln/npm:jquery
3. https://www.securityfocus.com/bid/102792/info

National Computer Security and Incident Response Team (Rw-CSIRT) Mission

Rw-CSIRT mission is to build cyber-security capabilities to increase the capacity of "early *Detection*, *Prevention*, *Response* to incidents and *Reduce* Vulnerability" and raise cyber security awareness in public.