**Alert – Google Chrome Security Updates**

**Description:**
Google Chrome is a web browser used to access the Internet. Google has released Chrome Version 72.0.3626.96 for Windows, Mac, and Linux. This release includes stability and performance improvements. This version addresses a critical vulnerability that an attacker could exploit to take control of an affected system.

**Overview and Impact of the vulnerabilities:**
Vulnerabilities have been discovered in Google Chrome, Successful exploitation of this vulnerabilities could allow an attacker to execute arbitrary code in the context of the browser. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

**Vulnerable or affected version:** Google Chrome versions prior to 72.0.3626.96

**Solutions (Mitigations):**

Rw-CSIRT is strongly recommending **users** to update their BROWSER to the latest versions by following the instructions below:

- Open your browser. Click the **Customize and control Google Chrome** button  in the upper-right corner of the screen.
- From the drop-down menu that appears, select **Help**, then select **About Google Chrome**.
- The window that appears will automatically check for updates and show you the current version of Chrome. If an update is available, Chrome will be updated automatically. After Chrome is updated, click the **RELAUNCH** option to restart Chrome and complete the update.

For **IT administrators** (managed environments):

- Apply stable channel update provided by Google to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

**Affected users should**: contact Rw-CSIRT by calling us on **4045** or writing to **security@risa.rw**

**References:**

https://chromereleases.googleblog.com/search/label/Stable%20updates

**Vulnerabilities Details:**

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-17480
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18342
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18343
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18349
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18350
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18355
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18356
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18357
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5754
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5755
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5756
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5757
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5758
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5759
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5760
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5761
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5762
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5763
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5764
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5765
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5766
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5767
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5768
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5769
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5770
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5771
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5772
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5773
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5774
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5775
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5776
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5777
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5778
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5779
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5780
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5781
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5782

**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.