Alert – Mozilla Firefox Security Updates

Description:
Mozilla Firefox is a web browser used to access the Internet. Mozilla Firefox ESR is a version of the web browser intended to be deployed in large organizations. Mozilla Firefox has released Version 65.0.1 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:
Multiple vulnerabilities have been discovered in Mozilla Firefox and Firefox Extended Support Release (ESR), the most severe of which could allow for arbitrary code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

Vulnerable or affected version:

- Mozilla Firefox versions prior to 65.0.1
- Mozilla Firefox ESR versions prior to 60.5.1

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 **menu** button ☰ , click ⓘ **Help** and select **About Firefox**.
- The **About Mozilla Firefox** window will open. Firefox will begin checking for updates and downloading them automatically.
- When the updates are ready to be installed, click **Restart to update Firefox**.

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

- Apply appropriate updates provided by Mozilla 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.

- Apply the Principle of Least Privilege to all systems and services.

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

References from Mozilla:
https://www.mozilla.org/en-US/security/advisories/mfsa2019-01/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-02/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-04/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-05/

Vulnerabilities Details from CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18335
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18356
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18511
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5785
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18500
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18501
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18502
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18503
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18504
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18505
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18506

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.