Firefox Releases Critical Patch Update to Stop Ongoing Zero-Day Attacks

Dear Constituents,

Mozilla has released Firefox 67.0.3 and Firefox ESR 60.7.1 versions to patch a critical zero-day vulnerability in the browsing software that hackers have been found exploiting in the wild.

How it Works

- A type confusion vulnerability can occur when manipulating JavaScript objects due to issues in `Array.pop`. This can allow for an exploitable crash.
- The vulnerability could allow attackers to remotely execute arbitrary code on machines running vulnerable Firefox versions and take full control of them.

Affected Operating System using Firefox

Those who use Firefox on desktop (Windows, macOS, and Linux) are more likely to be affected BUT for Firefox used by Android, iOS, and Amazon Fire TV are not affected.

What to do

- Through Firefox automatically installs latest updates and activate new version after a restart,
- users are still advised to ensure they are running the latest Firefox 67.0.3 and Firefox (Extended Support Release) 60.7.1 or later.

Reference

Firefox: https://www.mozilla.org/en-US/security/advisories/mfsa2019-18/

Pease for more information you can contact us:

Tonga National CERT
Ministry of MEIDECC
Nuku'alofa
Tel: 2378 (CERT)
email: cert@cert.gov.to
web: www.cert.gov.to

Disclaimer Notice:

The information in this notice is intended solely for public knowledge and awareness, and not intending to harm, fright or disturb any person(s), legal entity or the receiver of this information. Under no circumstances shall the Ministry of MEIDECC be liable for any indirect, incidental, consequential, special or exemplary damages arising out of or in connection with your access or use of or inability to access or use the information and any third party content and services