Google Chrome Vulnerability Advisory

Dear Constituents,

Google has released a report on a HIGH severity vunerability in CHROME that could allow the remote attackers to excute arbitrary code and take full control of the computers. The vulnerability named as the **use-after-free** affects the web browsing software for all operating system including Microsoft Windows, Apple macOS and Linux.

How it works

1. Fisrtly is the **FileReader** it's a standard API that has been designed to allow web applications to asynchronously read the contents of files (or raw data buffers) stored on a user's computer, using 'File' objects to specify the file or data to read.
2. Secondly is the **use-after-free vulnerability** is a class of memory corruption bug that allows corruption or modification of data in memory, enabling an unprivileged user to escalate privileges on an affected system or software.
3. So how it works is that the use-after-free vulnerability in the FileReader could enable unprivileged attackers to gain privileges on the Chrome web browser, allowing them to escape sandbox protections and run arbitrary code on the targeted system.
4. In exploiting this vulnerability the attacker tricking victims into just opening, or redirecting them to, a specially-crafted webpage without requiring any further interaction.

What to do

- A patch for the security vulnerability has already been released to its users in a stable **Chrome update 72.0.3626.121** for Windows, Mac and Linux operating system.
- Check for the version of Google Chrome you are using. Previous versions than 72.0.3626.121 are at risk.
- Make sure that CHROME is updated to the latest version.

Steps for updating CHROME for Desktop

1. On your computer, open Chrome.
2. At the top right, click **More**.
3. Click on About Chrome
4. Click **Update Google Chrome**. If you don't see this button, you're on the latest version.
5. Click Relaunch.

Steps for updating CHROME for Mobile phone

1. Open chrome and visit chrom://version to see the Chrome version.
2. If it's not updated then visit your app store and download the updated version.

Reference

EdgeSpot- https://blog.edgespot.io/2019/02/edgespot-detects-pdf-zero-day-samples.html

Please 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