Chrome Zero-Day Bug with Exploits in the Wild.

Dear Constituents,

Google has discovered and reported a high severity vulnerability, that could allow remote attackers to execute arbitrary code and take full control of the victim's computer. Google is aware of reports that an exploit for CVE-2019-13720 exists in the wild,

How it Works

- According to Security Research, Chrome highlights the issues on an use-after-free vulnerabilities, one affecting Chrome's audio component (**CVE-2019-13720**) while the other resides in the PDFium (**CVE-2019-13721**) library.
- The use-after-free vulnerability is a class of memory corruption issues that allows corruption or modification of data in the memory, enabling an unprivileged user to escalate privileges on an affected system or software.

What to do

- For those using Chrome Browser on Windows, Mac, and Linux Operating Systems it is highly recommended to update browser to the latest version 78.0.3904.87

Reference

Chrome: https://chromereleases.googleblog.com/2019/10/stable-channel-update-for-desktop_31.html

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

1   CERT Tonga adopts the Traffic Light Protocol

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