CERT-MU Security Alert

Date of Issue: 28 March 2022

Google Issues Urgent Chrome Update to Patch Actively Exploited Zero-Day Vulnerability

Severity: High

Description

A high severity vulnerability has been identified in Google Chrome browser and the vulnerability is being actively exploited in the wild. Tracked as CVE-2022-1096, the zero-day flaw relates to a type confusion vulnerability in the V8 JavaScript engine. The vulnerability exists because of type confusion errors and it arises when a resource (e.g., a variable or an object) is accessed using a type that is incompatible to what was originally initialized. This error could have serious consequences in languages that are not memory safe like C and C++, enabling a malicious actor to perform out-of-bounds memory access.

Google Chrome has released updates to address this vulnerability and CERT-MU advises users to apply the patches urgently.

Workarounds

Google Chrome users are highly recommended to update to the latest version 99.0.4844.84 for Windows, Mac, and Linux to mitigate any potential threats.

Users of Chromium-based browsers such as Microsoft Edge, Opera, and Vivaldi are also advised to apply the fixes as and when they become available.

More information about the update is available on:
https://thehackernews.com/2022/03/google-issues-urgent-chrome-update-to.html

Report Cyber Incidents

Let us unite together for a Safe Mauritian cyberspace during this crisis situation.

Report cyber security incident on the **Mauritian Cybercrime Online Reporting System (MAUCORS - http://maucors.govmu.org/)**

Contact Information

Computer Emergency Response Team of Mauritius (CERT-MU)
National Computer Board
Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info. : contact@cert.ncb.mu
Incident: incident@cert.ncb.mu
Website: http://cert-mu.org.mu
MAUCORS: http://maucors.govmu.org