CERT.tg: SECURITY ANNOUNCEMENT **Date**: 05/12/2022

Content Type	Description
Title	*Google Chrome, High-Severity Zero-Day Flaw Exploited in The Wild – Emergency Patch !!*
Id	*202212/Alert/07*
Code TLP	*White*
Risk Level	*High*
Application and service has been designed	***Google Chrome, Chromium-based browsers such as Microsoft Edge, Brave, Opera, and Vivaldi***
Version	- *All Version less than **108.0.5359.94** for Mac and Linux* - *All Version less than **108.0.5359.94/.95** for Windows*
Platform	***Windows, Linux and MacOS***
Update	- *Upgrade to version **108.0.5359.94** for MacOS and Linux* - *Upgrade to version **108.0.5359.94/.95** for Windows to mitigate potential threats.*
Summary	*In response to the active exploit of an open high-severity zero-day vulnerability (CVE-2022-4262) in the Chrome web browser, Google has released an emergency security patch to address the issue.*
Impacts	- *Successful exploitation of this zero-day bug leads to crashes of the browser by reading or writing memory out of buffer bounds.* - *The memory safety bugs can be triggered by a remote host, causing the ping program to crash.* - *It may be possible for a malicious host to trigger remote code execution in ping*
Detailed Description	*On Friday, December 2, 2022, Google has released an emergency security patch to address the issue of the vulnerability referred to as CVE-2022-4262.* *The vulnerability referred to as CVE-2022-4262 (CVSS score: 9.6) concerns **Type confusion in V8 in Google Chrome prior to 108.0.5359.94 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)**.*
Solutions	*Google has strongly recommended all users to immediately update their chrome in order to prevent any exploitation in the wild.* *Update your Chrome by following the simple steps that we have mentioned below:* - *First of all, you have to select the Chrome menu.* - *Then select the Help option.* - *After that, you have to select the About Google Chrome option.*

	- *Now, wait for a few seconds, as Chrome will now automatically detect and download if there is any update available.* *Users are recommended to upgrade to **version 108.0.5359.94** for **MacOS** and **Linux** and **108.0.5359.94/.95** for **Windows** to mitigate potential threats.* *Users of Chromium-based browsers such as **Microsoft Edge, Brave, Opera**, and **Vivaldi** are also advised to apply the fixes as and when they become available.*
Links for more details	*https://chromereleases.googleblog.com/2022/12/stable-channel-update-for-desktop.html* *https://gbhackers.com/google-chrome-high-severity-zero-day/amp/* *https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-4262*