UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00054

ACTIVE ZERO-DAY EXPLOIT IN GOOGLE CHROME

DATE ISSUED: 27th October 2020

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	[✓ MEDIUM]	EASY

OVERVIEW

Known to be under exploit in the wild, Google have released a patch to cover a memory corruption vulnerability in the FreeType font rendering library of the Chrome browser software. CVE-2020-1599

BREAKDOWN

Known as a heap buffer overflow, this flaw was reported to Project Zero, Googles internal security task force team, and acted upon swiftly. This type of buffer overflow attack allows portions of the buffer to be overwritten and allocated to the heap portion of the memory. This flaw is considered be high risk and the patches released additionally cover four other bugs. Rated as high risk, CVE-2020-1600 relates to "inappropriate implementation in Blink," as well as CVE-2020-16001 and CVE-2020-16002. The noted medium-level risk is CVE-2020-16003.

REMEDIATION STEPS

- Users should ensure the version of Google Chrome is 86.0.4240.111 and if not, update with the latest security patches from Google for Windows, Mac and Linux.

REFERENCES & RESOURCES

Google Blog:	https://chromereleases.googleblog.com/2020/10/stable-channel-update-for-desktop_20.html
Threatpost:	https://threatpost.com/google-patches-zero-day-browser/160393/