UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 00050

GOOGLE CHROME86 FIXES CRITICAL FLAWS

DATE ISSUED: 12th October 2020

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

OVERVIEW

The latest version of Google Chrome offers fixes for 35 security flaws and a new password manager that includes checks for account compromise, and is available across Windows, Mac, Android and iOS.

BREAKDOWN

Critical vulnerabilities addressed in this updated version of Google Chrome include an issue with the payment components as described in CVE-2020-15967 and a memory corruption flaw that could result in many outcomes including execution of arbitrary code or application crashes. Use-after-free flaws were the majority of the critical vulnerabilities being remediated with this new launch which means there is an attempt to access a service or process whenever it is "freed" including printing (CVE-2020-15971), audio (CVE-2020,15972), password manager (CVE-2020-15991) and WebRTC (CVE-2020-15969). Not all details regarding the vulnerabilities have been disclosed in the interest of protecting users who have not yet updated to the new version. The new password compromise detection feature enables Google to alert a user when it is suspected that their password has been compromised on a web site so is a handy feature to have, similar to their Password Checkup Extension.

REMEDIATION STEPS

- Disable system access to port 23/2323
- Increase access control via port 23/2323 by removing all surplus accounts and increasing administration account password complexity.
- Convert P2P networks to a centralised topology where possible.

REFERENCES & RESOURCES

Threatpost:	https://threatpost.com/google-chrome-86-critical-payments-bug-password-check/159938/
How to Geek	https://threatpost.com/google-chrome-86-critical-payments-bug-password-check/159938/
Computer World	https://www.computerworld.com/article/3211427/whats-in-the-latest-chrome-update.html