UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0306

GOOGLE CHROMES ZERO-DAY VULNERABILITY

DATE ISSUED: 17th April 2023

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	**MEDIUM**	EASY

OVERVIEW

Google has released an “out-of-bound” update that fixes a high-severity zero-day vulnerability in its Chrome web browser. It could allow an authenticated user to perform arbitrary code execution on comprised systems.

BREAKDOWN

Clement Lecigne of Google's Threat Analysis Group (TAG) discovered a zero-day vulnerability defined as Access to Resource Using an Incompatible Type (Type Confusion) issue in the V8 JavaScript Engine. This can enable threat actors to access out-of-bounds system memory, particularly in applications written in languages without memory safety, such as C and C++, and allow arbitrary code execution. A successful exploit of type confusion vulnerabilities would generally result in a browser crash or arbitrary code execution on compromised machines. The vulnerability tracked as CVE-2023-2033 affects Windows, Mac, and Linux systems. Further information regarding the bug is kept confidential until a majority of users have applied the available updates to bring them up to the latest version.

REMEDIATION STEPS

- Upgrade to version 112.0.5615.121 for Google Chrome on Windows, macOS, and Linux to mitigate potential threats.
- To update Chrome, click on the three vertical ellipses in the top right corner > Settings > About Chrome, where the browser will automatically check for updates.

REFERENCES & RESOURCES

The Bleeping Computer https://www.bleepingcomputer.com/news/security/google-chrome-emergency-update-fixes-first-zero-day-of-2023/

Google Chrome https://chromereleases.googleblog.com/2023/04/stable-channel-update-for-desktop_14.html