UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 00068

TWO MORE ZERO-DAY'S FOR GOOGLE CHROME

DATE ISSUED: 16th November 2020

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

OVERVIEW

Another update is required for Google Chrome users after the discovery of further zero-day exploits that allow unauthenticated and remote access to systems via the web. Both are under known active exploitation in the wild.

CVE-2020-16013 and CVE-2020-16017

BREAKDOWN

Following the zero-day exploits published in Cyber Guidance Issue 0054 in October 2020, this brings the total of recent Google Chrome exploits up to 5, affecting Windows, macOS and Linux versions of the browser. By creating a web page and luring a victim to the site, an attacker can trigger a use-after-free error to execute their code onto the user's system. The other is related to issues associated with security checks and handling of JavaScript and WebAssembly through the open-source V8 component, wherever it has been potentially inappropriately implemented. Both of these flaws are rated as critical by Google.

REMEDIATION STEPS

- Ensure Google Chrome is the latest version to prevent this attack-chain exploit
- Use endpoint protection and detection technologies to respond to suspicious local activity

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/2-zero-day-bugs-google-chrome/161160/
CVE Details:	https://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-15031/opec-1/Google-Chrome.html
We Live Security:	https://www.welivesecurity.com/2020/11/12/google-patches-two-new-zero-day-flaws-in-chrome/