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

CYBER GUIDANCE ISSUE 00092

WATERING-HOLE ATTACKS EXPLOIT FLAWS

DATE ISSUED: 18th January 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Google's Project Zero team have discovered a major hacking campaign against Chrome, Windows and Android flaws where various exploit chains have been carried out via watering-hole attacks.

BREAKDOWN

Watering hole attacks are carried out by targeting the website(s) most often visited by organisation employees or targeted groups where malicious code is injected to the site with the aim of infecting a company device. These attacks have involved Remote Code Execution (RCE) using the known Windows Zero Day flaw and chains known as "n-day" exploits in Android with the CVE for each listed below. After infection, payloads were downloaded and carried out actions such as recording fingerprinting information, location data, running processes and installed applications. A number of techniques and the abilities displayed in these known attacks suggest that the malicious actors executing them are highly skilled and well-practiced at carrying out these forms of attack.

CVE-2020-6418, CVE-2020-1020, CVE-2020-1020, and CVE-2020-1027.

REMEDIATION STEPS

- Apply patches to all affected systems issued by the associated vendor.
- Use anti-malware software to scan devices and check for any malicious or suspicious behaviours or unsolicited downloads.
- Be wary when visiting sites and check the address bar for anomalies, check the padlock is shown to verify the certificate of the website and never enter credentials after following a link – always type the website address into the address bar.
- Use network monitoring tools to alert against abnormal or suspicious network activity

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/hacks-android-windows-zero-day/163007/
Google Project Zero https://googleprojectzero.blogspot.com/2021/01/in-wild-series-android-post-exploitation.html