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

CYBER GUIDANCE ISSUE 0322

GOOGLE RELEASES 12 SECURITY UPDATES

DATE ISSUED: 29th May 2023

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Google Chrome has released a security update that includes 12 security fixes. The most severe of these vulnerabilities could allow an authenticated attacker to perform arbitrary code execution on behalf of the logged-on user.

BREAKDOWN

The security update released by Google addresses multiple vulnerabilities in its Google Chrome web browser. The most severe of these vulnerabilities could allow an authenticated user to perform arbitrary code execution. Depending on the privileges associated with the user, an attacker could install programs, manipulate data, or create new accounts with domain administrator privilege access. The impacted Google Chrome versions are before 113.0.5672.126/.127 for Windows and before 113.0.5672.126 for Mac and Linux.

REMEDIATION STEPS

- Upgrade to the latest Google Chrome versions to mitigate the risks.
- Perform application updates on enterprise assets through automated patch management on a regular basis.
- Practice the principle of Least Privilege Access by running software as a non-privileged user without administrative rights to minimise the effects of a successful attack.
- Regularly monitor the network to detect and respond to anomalous network activity.
- Apply policies to restrict the use of certain websites, block downloads/attachments, block JavaScript, or restrict browser extensions.

REFERENCES & RESOURCES

CIS Advisories https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2023-051