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

CYBER GUIDANCE ISSUE 00032

6 BUGS REVEALED IN WHATSAPP

DATE ISSUED: 5th September 2020

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	LOW	MEDIUM	HIGH

OVERVIEW

After revealing their dedicated security page in a bid to offer greater transparency to their users, Facebook owned WhatsApp have released information on six security vulnerabilities in their application.

BREAKDOWN

Some of these flaws were detected by the internal Bug Bounty Facebook program where others were found by staff and automated systems during security review of underlying code. The platform has made a pledge to its users that it will focus efforts on disclosing any future vulnerabilities and seeks to offer complete transparency. Of the more notable flaws, URL validation issues in Android versions of the software could have been triggered remotely in a sticker message to any recipient containing malware without interaction from the user at all CVE-20020-1890 and Cross Site Scripting (XSS) could be allowed if a user accessed a URL in a live location message due to input validation CVE-2020-11928

REMEDIATION STEPS

- Update to the latest version of WhatsApp via reputable app store such as Google Play and Apple Store

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/whatsapp-discloses-6-bugs-dedicated-security-site/158962/

WhatsApp: https://www.whatsapp.com/security/