NCIS CYBER DIRECTORATE

WhatsApp Vulnerabilities Make User Information Vulnerable to Exposure and Manipulation

Security researchers have revealed several vulnerabilities within WhatsApp, highlighting the ability for malicious cyber actors to spy on victims, and access sensitive data.

WhatsApp is a free desktop or mobile application that allows users to perform a variety of functions to include sending and receiving secure messages, voice calls, user location, images, and videos. The app is used worldwide, with more than 1 billion users in over 180 countries. While the company continues to release patches, newly discovered vulnerabilities can leave WhatsApp users susceptible to cyberattacks.

- In August 2019, malicious cyber actors used WhatsApp to send phishing messages to victims. The messages appeared to originate from Instagram and requested the user to provide their Instagram password in order to keep their account active. When the victim entered a valid password, the cyber actors were able to log in to the victim's Instagram account and change the email address associated with the account. Once the cyber actors gained access to the victim's Instagram ID and password, they were able to navigate to the victim's Gmail account and attempt to take over that account as well; however, Google's security features and two-factor authentication prevented the cyber actors from further accessing the victim's email account.
- In July and August 2019, security researchers revealed several attack methods in which WhatsApp could be exploited to allow cyber actors to intercept, manipulate, and expose photos, videos, documents, and voice recordings, to spread false information to other users. The methods used include altering the victim's settings and permissions within the WhatsApp application to set "private" messages as "public", change the identity of the sender, and alter message content.
- Between May and August 2019, security researchers revealed several attack methods in which WhatsApp could be exploited to intercept, manipulate, and disclose personal information of users, gather credentials to access additional accounts belonging to the users, and remotely deliver spyware to victims.

Vulnerabilities in popular social networking apps such as WhatsApp, can be used as an effective method of gaining access to the victim's device, information, and additional accounts that may be linked. To assist in mitigating mobile malware threats, users are encouraged to remain aware of app permissions and settings, and only allow apps to access functions that are necessary for that specific app. Additional mitigation techniques include checking for updates as patches are released, deleting unwanted apps, verifying the sender of messages and device notifications prior to clicking on them, enabling two-factor authentication on accounts when possible, and remaining vigilant for any unusual behavior the device may display.

WWW.NCIS.NAVY.MIL

OCTOBER 2019
CYBERSECURITY AWARENESS MONTH