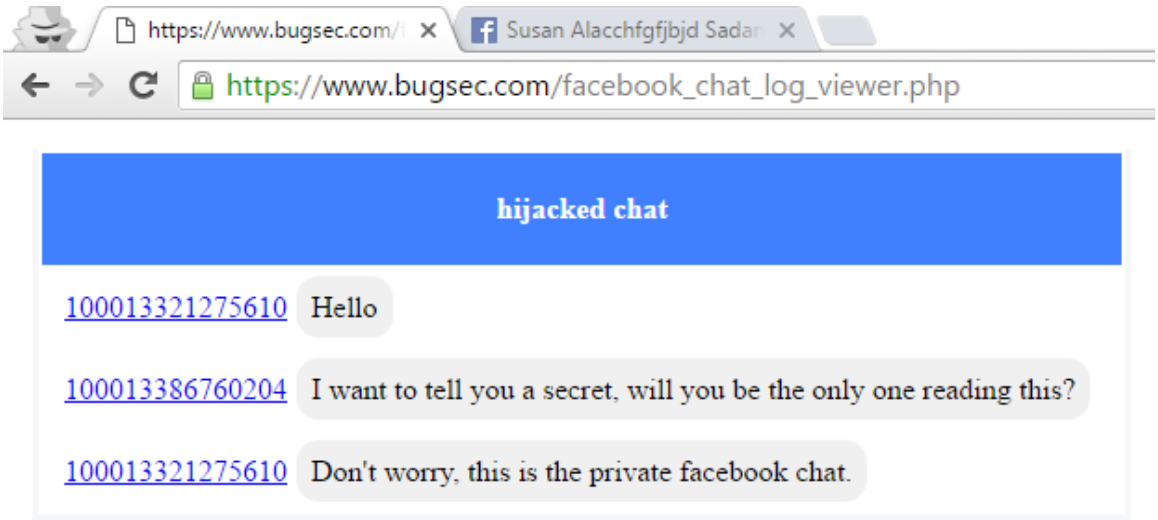
BugSec, Cynet Discover Critical Vulnerability Affecting Privacy of 1-Billion Facebook Messenger Users

'Originull' security flaw allows hackers to read messages, view photos sent via web and mobile chat; potentially affects millions of websites using origin restriction checks

TEL AVIV, ISRAEL — Tuesday, December 13, 2016

BugSec Group Ltd., a leading provider of offensive and defensive security consulting services (www.bugsec.com), and Cynet, pioneers of the advanced threat detection and response platform (www.cynet.com), announced today the discovery of the 'Originull' privacy hack, a severe security vulnerability on Facebook Messenger that could also potentially affect millions of websites that use origin restriction checks. The vulnerability, identified by researcher Ysrael Gurt, allows attackers to read messages and view photos and other attachments sent by Messenger both from the web and from the mobile application. It was disclosed to Facebook via their Bug Bounty program; the Facebook security team investigated and repaired the flawed component.



The root of the vulnerability was a cross-origin problem in Facebook's implementation, which would allow an attacker to bypass Facebook's origin checks and access messages from an external website.

"This security flaw meant that the messages of 1-billion active monthly Messenger users were vulnerable to attackers," said Stas Volfus, Chief Technology Officer of BugSec.

To exploit the vulnerability, the victim would have to visit a malicious website controlled by the attacker. From that moment, all messages sent or received by the victim would be accessible to the attacker.

Said Volfus, “This was an extremely serious issue, not only due to the high number of affected users, but also because even if the victim sent their messages using another computer or mobile, they were still completely vulnerable. Facebook realized the potential severity, and responded quickly, verifying the flaw and fixing it.”

The heart of the issue lies in the fact that Facebook Messenger chats are managed from a separate server located at the address: {number}-edge-chat.facebook.com. The chat itself runs on the domain www.facebook.com.

Communication between the JavaScript and the server is done by XML HTTP Request (XHR). In order to access the data that arrives from 5-edge-chat.facebook.com in JavaScript, Facebook must add the “Access-Control-Allow-Origin” header with the caller’s origin, and the “Access-Control-Allow-Credentials” header with “true” value, so that the data is accessible even when the cookies are sent.

However, when the server received a GET request to the chat domain, it would not include the “origin” header. In many development languages, nonexistent headers are represented by the “null” value in place of the requested header. If Facebook expected to receive “null” in the “origin” header, it would not block requests from this “origin.”

To see full details of the vulnerability, read the blogpost at https://www.bugsec.com/news/facebook-originull/ or http://www.cynet.com/blog-facebook-originull/.

For expert advice on cyber-attack simulation and penetration testing, contact BugSec at info@bugsec.com.

To learn more about advanced threat detection and response, contact Cynet at info@cynet.com.

About BugSec

BugSec Group is a leading offensive and defensive security consulting company, focused on ethical hacking, security research, cyber-attack simulations, SCADA, Incident Response, product security evaluation and other services to increase customer security. Since 2005, BugSec has been providing security consulting services to global companies in the fields of finance, defense, government, hi-tech, utilities and other markets. The BugSec team is made up of some

of the world's most talented offensive and defensive hacking experts and security research teams, who work together with intelligence and law enforcement organizations around the world to help our customers protect their assets.
www.bugsec.com

Follow BugSec at:
Facebook: www.facebook.com/bugsec
Twitter: www.twitter.com/bugsec_group
LinkedIn: www.linkedin.com/bugsec

About Cynet
Cynet is a leader in advanced threat detection and response. Cynet simplifies security by providing a scalable, easily deployable protection platform that delivers prevention, precise findings and automated response to advanced threats with near-zero false positives, shortening the time from detection to resolution and limiting damage to an organization. Cynet's unique visibility of files, users, network traffic, and endpoints, and continuous monitoring of the environment, uncovers behavioral and interaction indicators across the attack chain, giving a complete picture an attack operation over time. Cynet is enhanced by Cynet CyOps, which delivers additional value to the platform with 24/7 threat expert assistance, insight and intelligence. By combining high fidelity detections, decoy interactions, network analytics, and expert analyst assistance, Cynet provides accurate findings with associated risks without a lot of complexity and noise, so security teams can prioritize and respond to what matters.
www.cynet.com

Follow Cynet at:
Facebook: www.facebook.com/cynet360
Twitter: www.twitter.com/cynet360
LinkedIn: www.linkedin.com/cynet-security

Press Contact:
Inbal Aharoni
Marketing Manager
Mobile: +972-508776797
Email: inbala@cynet.com

###