UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 00028

SLACK RCE BUG

DATE ISSUED: 31st August 2020

IMPACT	LOW	[✓ MEDIUM]	HIGH
EASE OF EXPLOIT	[✓ LOW]	MEDIUM	HIGH

OVERVIEW

Affecting version 4.4 of the Slack desktop application, this critical vulnerability allows Remote Code Execution (RCE) where attackers can gain full control and have access to private conversations, channels, passwords, tokens, and keys among other functions.

BREAKDOWN

Using Cross Site Scripting (XSS) and HTML injection, attackers may exploit version prior to 4.4 on Mac, Windows and Linux devices to gain full control of the user's application and associated account. Depending on the application configuration there is also the potential for an attacker to move into another network. Exploitation may be triggered by overwriting the "env" function and creating a tunnel through BrowserWindow and the execution of arbitrary code such as JavaScript. The attacker would upload their payload to their own HTTPS-enabled server and prepare a post containing the URL pointing to their malicious code, often hidden in an image. Once this post is uploaded to a channel or sent to another user, if the user accesses the image the hidden code will execute on their computer. Although there are protections in JavaScript through the Content Security Policy (CSP), it is possible to circumvent these using element such as map tags to hide the URL for the "one-click" RCE. Additionally, plaintext emails are stored on Slack servers that are unfiltered and may be used in the stead of the self-hosting of the malicious URL and abused as a phishing platform. Further development may lead to the malware evolving into a worm in order to self-propagate to other systems.

REMEDIATION STEPS

- Practice caution when accepting messages from or accessing public posts from unknown servers
- Use anti-malware software for detect and response actions for unusual system activity
- Update Slack application to the latest version
- Use URL filtering to prevent access to malicious sites

REFERENCES & RESOURCES

Threatpost:	https://threatpost.com/critical-slack-bug-access-private-channels-conversations/158795/
Dark Reading:	https://www.darkreading.com/vulnerabilities---threats/slack-patches-critical-desktop-vulnerability/d/d-id/1338797
Computing.co.uk	https://www.computing.co.uk/news/4019563/slack-fixes-critical-rce-bug-desktop-app