March 7, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- New Security Vulnerability Affects Thousands of GitLab Instances.
- Chrome Skype extension found to be leaking user info.
- LFI/RCE vulnerability found in Hashnode
- Critical Bugs Reported in Popular open source PJSIP SIP and Media Stack
- Critical Vulnerabilities Impact Widely Used Printed Circuit Board File Viewer

CryptoGen Nepal

Introduction to InfoSec Weekly

InfoSec Weekly is a compilation of security related news feed that aims to update the readers about cyber security, cyber threats, malware attacks, new technologies and cyber security awareness every week. We primarily cover events and news related to offensive side of the Information Security such as hacking, password and sensitive information leakage, new vulnerabilities and important CVE's that can impact an individual or an organization. We also aim to provide defensive tactics to overcome known vulnerabilities that can protect organizations and individuals from any attacks.

Our main aim is to spread awareness regarding various cyber related threats.

About Us

We are a team of security enthusiasts with an aim to provide various Information Security Services to organizations. Our company aims to provide professional grade cyber security solutions for all your Information Technology infrastructures. Our team has been demonstrating penetration testing skills using methodologies such as OSSTMM, NIST and OWASP. We aim to help companies protect their valuable data from any internal or external threats. Our team members have been practicing their skills to detect and report vulnerabilities in a live environment. Organizations such as Google, Facebook, Twitter, Yahoo!, eBay, eset, BugCrowd, under armour, Coinbase, CCM, etc. have recognized our team members for reporting vulnerabilities and have helped these organizations from malicious users. Our team's professional work experience consists of various Government organizations, National and International based private organizations, INGOs, etc. Our Services ranges from VAPT, Incident Response, Information Security Training, Endpoint threat analysis, Cyber security consultant, etc.

New Security Vulnerability Affects Thousands of GitLab Instances.

Description

Researchers have discovered a newly patched security vulnerability in GitLab. This GitLab is open-source DevOps software that could possibly expose sensitive information to a remote, unauthenticated user. All versions of GitLab Community Edition and Enterprise Edition from 13.0 to 14.8 are affected by the medium-severity bug. On November 18,2021, Jake Banis founded this vulnerability disclosure. The flaw arises from a failure to perform an authentication check while using the GitLab GraphQL API. This vulnerability can be used by a remote, unauthenticated attacker to obtain registered GitLab identities, names, and email addresses.

Source	https://thehackernews.com/2022/03/new-security-vulnerability-affects.html
Infected Technology	GitLab open-source DevOps software.
Recommendation	Upgrade to the new version of GitLab packages.
CVE_ID	CVE-2021-4191 CVE-2022-0735

Chrome Skype extension found to be leaking user info.

Description

Microsoft has solved a privacy flaw in its Skype extension for Chrome that put millions of users' account information at risk. The issue, according to the researcher, was in the extension's identity-tracking capabilities, which could tell whether a user was logged into a Microsoft account. He discovered that the user identifier was executed in the content script of the extension. He did, however, point out that "in a content script context, "sessionStorage" is no longer the extension's storage, but in the website's storage." As a result, the website can read it out trivially."

Source	https://portswigger.net/daily-swig/private-chat-chrome-skype-extension-with-9m-installs-found-to-be-leaking-user-info
Infected Technology	All versions of skype extension before the March update.
Recommendation	Disable the skype extension from web browser or update it to the latest patch.

LFI/RCE vulnerability found in Hashnode

Description	
Hashnode is a popular blogging platform for developers. On February 28, Security researchers Aditya Dixit and Adhyayan Panwar disclosed an RCE exploit caused by LFI (Local file inclusion) bug present in the platform's bulk markdown importer. After discovering an LFI the pair were able to download sensitive files from the web server (such as the /etc/passwd, /proc/net/tcp) and also gain SSH keys (from ~/.ssh).	
Source	https://blog.dixitaditya.com/pwning-a-server-using-markdown
Infected Technology	Hashnode blogging platform
Recommendation	The vulnerability was disclosed privately to Hashnode and has been patched already. The ssh keys have also been rotated.

Critical Bugs Reported in Popular open source PJSIP SIP and Media Stack

Description	
Many security vulnerabilities have been disclosed in PJSIP open-source multimedia communication library that could be abused by an attacker to trigger arbitrary code execution and denial-of-service (DoS) in applications that use the protocol stack. PJSIP is an open-source embedded SIP protocol suite written in C that supports audio, video, and instant messaging features for popular communication platforms such as WhatsApp and Blue Jeans. The flaws effected Stack overflow, Read out-of-bounds, Buffer overflow in PJSUA API when calling pjsua_recorder_create(), pjsua_playlist_create(), pjsua_call_dump()	
Source	https://thehackernews.com/2022/03/critical-bugs-reported-in-popular-open.html
Infected Technology	Open Source PJSIP SIP and Media Stack
Recommendation	Enable a malicious actor to pass attacker-controlled arguments to any of the vulnerable APIs and update latest version.
CVE_ID	CVE-2021-43299, CVE-2021-43300, CVE-2021-43301, CVE-2021-43302, CVE-2021-43303

Critical Vulnerabilities Impact Widely Used Printed Circuit Board File Viewer

Description	
Six critical vulnerabilities were disclosed affecting Gerbv, an open source file viewer for printed circuit board(PCB) designs. PCB manufactures uses software like Gerbv in their web interfaces as a tool to convert Gerber files into images. The uploaded files which are converted to an image to be displayed in a browser, so that user can verify that matches their expectations this helps attacker to reach the software over network without user interaction or elevated privileges. Till now patches of four vulnerabilities have been released while two vulnerabilities still remain unpatched.	
Source	https://www.securityweek.com/critical-vulnerabilities-impact-widely-used-printed-circuit-board-file-viewer
Infected Technology	Gerbv A native Linux application.
Recommendation	Update to latest version
CVE_ID	CVE-2021-40391, CVE-2021-40393, CVE-2021-40394, CVE-2021-40401, CVE-2021,40400 and CVE-2021-40402

For any queries/recommendations:
Contact us: **whois@cryptogennepal.com**

OUR SERVICES

Our services as information security company includes:

- INFORMATION SECURITY AUDIT
- VULNERABILITY ASSESSMENT
- PENETRATION TESTING
- MANAGED/CO.MANAGED SOC
- INCIDENT RESPONSE
- THREAT ANALYSIS
- SERVER HARDENING
- CYBER SECURITY CONSULTANT
- INFORMATION SECURITY TRAINING