April 4, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Spring Cloud framework commits patch for code injection flaw
- QNAP Warns of OpenSSL Infinite Loop Vulnerability Affecting NAS Devices
- Apple issues patch for 2 activity exploited 0-days in iPhone, iPad, and Mac Devices
- HTML parser bug triggers Chromium XSS security flaw
- SQL injection leading to unauthenticated RCE in ImpressCMS

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.

Spring Cloud framework commits patch for code injection flaw

Description

On March 28 a vulnerability was detected in Spring Cloud Function which allows attacker to “provide a specially crafted Spring Expression Language” which may result in access to local resources” As per NSFOCUS, the vulnerability is triggered by the spring.cloud.function.routing-expression in the request header and is processed as a SpEL expression when routing is used. Through this expression the attacker may be able to access server-side content, tamper with functionality, hijack accounts or more.

Source	https://portswigger.net/daily-swig/spring-cloud-framework-commits-patch-for-code-injection-flaw
Infected Technology	Spring Cloud
Recommendation	Update to latest version
CVE_ID	CVE-2022-22963

QNAP Warns of OpenSSL Infinite Loop Vulnerability Affecting NAS Devices

Description

QNAP, said this week that a weakness in the open-source OpenSSL cryptographic library has compromised a small number of its network-attached storage (NAS) machines. Certain QNAP NAS have been discovered to be vulnerable to an endless loop issue in OpenSSL. The vulnerability can be used to launch denial-of-service attacks if it is exploited. The problem is caused by a defect that occurs during parsing security certificates, causing a denial-of-service scenario and crashing unpatched devices remotely. The announcement comes a week after QNAP issued security upgrades for QuTS hero (version h5.0.0.1949 build 20220215 and later) to solve the "Dirty Pipe" local privilege escalation bug that affected the company's devices.

Source	https://thehackernews.com/2022/03/qnap-warns-of-openssl-infinite-loop.html
Infected Technology	QTS and QuTScloud operating systems
Recommendation	Patches are expected to be released soon.
CVE_ID	CVE-2022-0778

Apple issues patch for 2 activity exploited 0-days in iPhone, iPad, and Mac Devices
Description
Apple released emergency patches for two zero-day flaws in its mobile and desktop operating systems on Thursday, claiming that they have been exploited in the wild. The shortcomings have been fixed as part of updates to iOS and iPadOS 15.4.1, macOS Monterey 12.3.1, tvOS 15.4.1, and watchOS 8.5.1. Because the flaws are being actively exploited, Apple iPhone, iPad, and Mac users are strongly advised to update to the most recent versions of the software as soon as possible to avoid any threats.

Source	https://thehackernews.com/2022/03/apple-issues-patches-for-2-actively.html
Infected Technology	iOS, iPadOS, macOS, tvOS, watchOS
Recommendation	Update to the latest version of OS.
CVE_ID	CVE-2022-22675

HTML parser bug triggers Chromium XSS security flaw
Description
The Security flaw was found in the Chromium source code's tree builder. HTML is initially parsed with "html_tree_builder" and then the result is parsed with "html_tree_builder_simulator". Resulting in discrepancy which triggered the XSS vulnerability. According to the researchers, When the content was passed in the Second DOM tree, an image tag was included outside of the original parse, leading to XSS.

Source	https://portswigger.net/daily-swig/html-parser-bug-triggers-chromium-xss-security-flaw
Infected Technology	Chromium version below 99.0.4844.51
Recommendation	Update to latest Chromium version
CVE_ID	CVE-2022-0801

SQL injection leading to unauthenticated RCE in ImpressCMS	
Description	
The latest version of the popular content management system (CMS), ImpressCMS, contains SQL injection vulnerability which can be leveraged to achieve remote code execution (RCE). According to threat researcher Egidio "Egix" Romano, the RCE flaw should only be exploitable by registered ImpressCMS users, however, a 'new' SQL injection technique could be used to bypass the Protector. Protector is ImprcessCMS's Web Application Firewall (WAF). However, for the attack to be successful, there must be PDO database driver installed and exectuion of stacked SQL queries must be supported.	
Source	https://portswigger.net/daily-swig/sql-injection-protections-in-impresscms-could-be-bypassed-to-achieve-rce
Infected Technology	ImpressCMS (before version 1.4.2)
Recommendation	Update to latest patches as soon as possible.
CVE_ID	CVE-2022-26599

New Spring Java framework zero-day allows remote code execution	
Description	
Unauthenticated remote code execution on applications is possible because to a new zero-day vulnerability in the Spring Core Java framework termed 'Spring4Shell.' Spring is a well-known application framework that enables software developers to create Java applications with enterprise-level functionality fast and efficiently. These apps can then be deployed as stand-alone packages, complete with all essential dependencies, on servers such as Apache Tomcat. CVE-2022-22963 has been assigned to a new Spring Cloud Function Zero-day vulnerability.	
Source	https://www.bleepingcomputer.com/news/security/new-spring-java-framework-zero-day-allows-remote-code-execution/
Infected Technology	Spring Framework of Java.
Recommendation	Spring applications deploy properly and update newer versions of spring framework.
CVE_ID	CVE-2022-22963

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

CryptoGen Nepal

https://www.facebook.com/CryptoGenNepal/
https://twitter.com/CryptoGenNepal
https://www.instagram.com/CryptoGenNepal/