June 20, 2022

# INFOSEC WEEKLY

## #MADE4SECURITY

Cisco says it won’t fix zero-day RCE in end-of-life VPN routers

Exploited Vulnerability Patched in WordPress Plugin with Over 1 Million Installations

GhostTouch: Hackers can reach your phone’s touchscreen without even touching it

High-Severity RCE vulnerability present in Fastjson Library

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.

## Cisco says it won’t fix zero-day RCE in end-of-life VPN routers

| **Description** | |
|---|---|
| This vulnerability affecting only devices with the web-based remote management interface enabled on WAN connections. This vulnerability has a CVSS severity rating of 9.8 out of 10. The flaw exists due to insufficient user input validation of incoming HTTP packets on the impacted devices. Using this vulnerability attacker could exploit by sending a specially crafted request to the web-based management interface, resulting in command execution with root-level privileges. | |
| Source | https://www.bleepingcomputer.com/news/security/cisco-says-it-won-t-fix-zero-day-rce-in-end-of-life-vpn-routers/ |
| Infected Technology | Cisco RV routers |
| Recommendation | • Update to newer models |
| CVE_ID | CVE-2022-20825 |

## Exploited Vulnerability Patched in WordPress Plugin with Over 1 Million Installations

| **Description** | |
|---|---|
| Ninja Forms plugin vulnerability that appears to have been exploited in the wild on more than one million WordPress websites. This vulnerability helps administrators add customizable forms to their WordPress sites. One potentially critical exploit chain in particular involves the use of the NF_Admin_Processes_ImportFrom class to achieve remote code execution via deserialization, through there would need to be another plugin or theme installed on the site with a usable gadget. | |
| Source | https://www.securityweek.com/exploited-vulnerability-patched-wordpress-plugin-over-1-million-installations |
| Infected Technology | WordPress Plugin |
| Recommendation | • Update to latest version |

| GhostTouch: Hackers can reach your phone’s touchscreen without even touching it | |
|---|---|
| **Description** | |
| Capacitive touchscreens of today's smartphones and tablets allow for multi-touch and the measurement of tiny electric fields. Capacitive touchscreens, on the other hand, are susceptible to the effects of electromagnetic interference (EMI) and charger noise. Previous research has shown that EMI may disturb the touchscreen user experience and perhaps generate unpredictable and dangerous behavior. Because of EMI signals, a phone that was left on a charger once booked an extremely costly hotel stay. The researchers intended to test if they could utilize EMI to produce programmable touch events and initiate arbitrary behavior on capacitive touchscreens when they created GhostTouch. Electromagnetic interference (EMI) and charging noise in the surroundings. The main concept of GhostTouch is to use electromagnetic pulses injected into the receiving electrodes embedded into the touchscreen to interfere with capacitance measurements. | |
| Source | https://portswigger.net/daily-swig/ghosttouch-hackers-can-reach-your-phones-touchscreen-without-even-touching-it |
| Infected Technology | Any Smart phones with touch screen capability |
| Recommendation | • No update yet. Stay up to date with security news |
| CVE_ID | CVE-2022-20825 |

## High-Severity RCE vulnerability present in Fastjson Library

**Description**

Fastjson is a Java library that is used to convert Java objects into their JSON representation and vice versa. Cybersecurity researchers from JFrog disclosed a recently patched high-severity vulnerability that can potentially be exploited to achieve remote code execution (RCE). Uriya Yavnieli said “This vulnerability affects all Java applications that rely on FastJson versions 1.2.80 or earlier and that pass user-controlled data to either the JSOn.parse or JSON.parseObject APIs without specifying a specific class to deserialize.”

| | |
|---|---|
| Source | https://thehackernews.com/2022/06/high-severity-rce-vulnerability.html |
| Infected Technology | Fastjson library |
| Recommendation | • Update to version 2.1.83 |
| CVE_ID | CVE-2022-25845 |

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/