April 18, 2022

# INFOSEC WEEKLY

## #MADE4SECURITY

- Git Security Vulnerabilities Which Can Lead to Execution of Arbitrary Commands.
- Spring4Shell Vulnerability Used by Hackers to Deploy Mirai Botnet Malware
- Critical infrastructure entities on red alert over 'exceptionally rare and dangerous' ICS malware
- Critical Auth Bypass Bug Reported in Cisco Wireless LAN Controller Software
- JekyllBot:5 allow hackers to control Aethon TUG Hospital Robots.

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.

## Git Security Vulnerabilities Which Can Lead to Execution of Arbitrary Commands.

| **Description** | |
|---|---|
| Windows users are at highest risk from security bugs in software development tool. This issue affects users on multi-user machines, where malicious attacker might build a ".git" directory in a shared location above the victim's current working directory, which would force any git invocations outside of a repository to read the set values. The Git for Windows uninstaller is vulnerable to a second vulnerability (CVE-2022-24767). As with the prior weakness, some amount of compromised access is required for prospective attacks, according to GitHub's notice. Attacks would rely on the installation of malicious.dll files on a target machine. | |
| Source | https://portswigger.net/daily-swig/git-security-vulnerabilities-prompt-updates |
| Infected Technology | Git Version below 2.35.2 |
| Recommendation | Upgrade the Git version to 2.35.2 |
| CVE_ID | CVE-2022-24765, CVE-2022-24767 |

## Spring4Shell Vulnerability Used by Hackers to Deploy Mirai Botnet Malware

| **Description** | |
|---|---|
| Since the beginning of April 2022, threat actors have been actively exploiting the recently reported major Spring4Shell vulnerability to execute the Mirai botnet malware, mainly in the Singapore region. "Through the exploitation, threat actors can download the Mirai sample to the '/tmp' folder and run it after changing permissions with 'chmod,'" says the report. Malicious actors could exploit the flaw to get remote code execution in Spring Core applications in non-default settings, giving them complete control over the infected devices. | |
| Source | https://thehackernews.com/2022/04/hackers-exploiting-spring4shell.html |
| Infected Technology | Spring Core Application (Java) |
| Recommendation | Regular inspection of the software is needed for evidence of exploitation. |
| CVE_ID | CVE-2022-22965 |

## Critical infrastructure entities on red alert over 'exceptionally rare and dangerous' ICS malware

| **Description** | |
|---|---|
| The warning was issued by US government about advance persistent threat actors having fashioned tools capable of hijacking industrial devices deployed in critical infrastructures sectors. The tools enables criminals "to scan for, compromise, and control affected devices once the initial access to the operational technology (OT) network". The actors can leverage the modules to scan for targeted devices, conduct reconnaissance on device details, upload malicious configuration/code to targeted device, backup or restore device contents, and modify device parameters. | |
| Source | https://portswigger.net/daily-swig/critical-infrastructure-entities-on-red-alert-over-exceptionally-rare-and-dangerous-ics-malwar |
| Infected Technology | ASRock-signed motherboard driver, AsrDrv103.sys |
| Recommendation | Having defensible architecture, network monitoring and specific incident response plan. |
| CVE_ID | CVE-2020-15368 |

## JekyllBot:5 allow hackers to control Aethon TUG Hospital Robots.

| **Description** | |
|---|---|
| Security firm, Cynerio, discovered five zero-day vulnerabilities that enable hackers to access Aethon Tug hospital robots remotely. The vulnerabilities are collectively dubbed 'JekyllBot:5'. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) said "Successful exploitation of these vulnerabilities could cause denial-of-service conditions, allow full control of robot functions, or expose sensitive information." A malicious actor could weaponize the vulnerabilities and pivot further into the internal hospital network and surveil individuals and primacies, and gain unauthorized access to confidential information. | |
| Source | https://thehackernews.com/2022/04/new-jekyllbot5-flaws-let-attackers-take.html |
| Infected Technology | TUG Hospital autonomous robots by Aethon. |
| Recommendation | Update and path firmware and software as soon as they are available. |
| CVE_ID | CVE-2022-1070, CVE-2022-1066, CVE-2022-26423, CVE-2022-27494, CVE-2022-1059 |

## Critical Auth Bypass Bug Reported in Cisco Wireless LAN Controller Software

| **Description** | |
|---|---|
| Cisco has addressed a significant security flaw in the Wireless LAN Controller (WLC) that may allow an unauthenticated, remote attacker to take control of a system. The severity of the problem is a ten out of ten, and it allows an adversary to overcome authentication measures and log in to the device using the WLC administration interface. The password validation mechanism was implemented incorrectly, resulting in this vulnerability. An attacker might take advantage of this flaw by using modified credentials to log into an affected device. An attacker might get administrator access and carry out harmful operations that allow a complete takeover of the affected system if the bug is successfully exploited. | |
| Source | https://thehackernews.com/2022/04/critical-auth-bypass-bug-reported-in.html |
| Infected Technology | Wireless LAN Controller (WLC) (3504 WC, 5520 WC, 8540 WC) |
| Recommendation | Update to the latest version |
| CVE_ID | CVE-2022-20695 |

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

z