



# October 18, 2021

## INFOSEC WEEKLY

#MADE4SECURITY

- Juniper Networks Patches Over 70 Vulnerabilities
- GitHub Actions Flaw allows Code Review Bypass
- Apple releases patches for zero-day vulnerabilities
- Linphone and MicroSIP critical remote hacking flaws
- Chrome Ad-Blocker extension caught injecting Ads



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.

---

## Juniper Networks Patches Over 70 Vulnerabilities

### Description

Juniper Networks has issued security patches to address vulnerabilities in a variety of products. An attacker might exploit some of these flaws to gain control of a vulnerable system. Remote code execution issues, privilege escalation, DoS vulnerabilities, and XSS are among the flaws addressed by the firm. Many of the issues are introduced by the use of third-party components. The majority of the security flaws affect Juniper's Junos OS operating system, which is used by many of the company's products.

Source	<a href="https://kb.juniper.net/InfoCenter/index?page=content&amp;channel=SECURITY_ADVISORIES&amp;cat=SIRT_1&amp;actp=&amp;sort=datemodified&amp;dir=descending&amp;max=1000&amp;batch=15&amp;rss=true&amp;itData.offset=0">https://kb.juniper.net/InfoCenter/index?page=content&amp;channel=SECURITY_ADVISORIES&amp;cat=SIRT_1&amp;actp=&amp;sort=datemodified&amp;dir=descending&amp;max=1000&amp;batch=15&amp;rss=true&amp;itData.offset=0</a>
--------	---

Infected Technology	Juniper Products
---------------------	------------------

Recommendation	Update the latest available patch
----------------	-----------------------------------

---

## GitHub Actions Flaw allows Code Review Bypass

### Description

Cider Security researchers have identified loophole in GitHub Actions that allows threat actors to bypass reviews mechanism and push non-reviewed code to protected branch. The exploitation of the flaw is not recorded however the issue is not fixed.

Source	<a href="https://medium.com/cider-sec/bypassing-required-reviews-using-github-actions-6e1b29135cc7">https://medium.com/cider-sec/bypassing-required-reviews-using-github-actions-6e1b29135cc7</a>
--------	---

Infected Technology	GitHub
---------------------	--------

Recommendation	Disable GitHub Action if not in use Enable multiple approval to merge pull request
----------------	---

---

## Apple releases patches for zero-day vulnerabilities

### Description

Apple addressed a critical vulnerability that is claimed to be exploited in the wild. Only this year, there has been 17 zero-day flaw the company has addressed. The issue seems to be a memory corruption issue in the "IOMobileFrameBuffer" component that could allow an application to execute arbitrary code with kernel privileges.

Source	<a href="https://support.apple.com/en-us/HT212846">https://support.apple.com/en-us/HT212846</a>
--------	---

Infected Technology	Apple iPhone and iPad
---------------------	-----------------------

Recommendation	Update your iphone and ipad to latest patch iOS 15.0.2 and iPadOS 15.0.2
----------------	--

CVE	CVE-2021-30883
-----	----------------

---

---

## Linphone and MicroSIP critical remote hacking flaws

### Description

New multiple security vulnerabilities have been disclosed in softphone software from Linphone and MicroSIP that could be exploited by an unauthenticated remote adversary to crash the client and even extract sensitive information like password hashes by simply making a malicious call. Softphones are software-based phones that work like desk phones where users can make telephone calls over the Internet.

Source	<a href="https://thehackernews.com/2021/10/critical-remote-hacking-flaws-disclosed.html">https://thehackernews.com/2021/10/critical-remote-hacking-flaws-disclosed.html</a>
--------	---

Infected Technology	Linphone and MicroSIP
---------------------	-----------------------

Recommendation	Update patches on Linphone and MicroSIP softwares
----------------	---

CVE	CVE-2021-33056
-----	----------------

---

---

## Chrome Ad-Blocker extension caught injecting Ads

### Description

A chrome and Opera web browser ad blocker extension are found inserting ads and affiliated code on websites. The findings come following the discovery of rogue domains distributing an ad injection script. The extension is said to earn money when specific actions like registration or sale of the product take place. The imperva researcher mentions that this could be part of a larger distribution campaign with ties to a previous PBot campaign

Source	<a href="https://www.imperva.com/blog/the-ad-blocker-that-injects-ads/">https://www.imperva.com/blog/the-ad-blocker-that-injects-ads/</a>
Infected Technology	AllBlock Chrome and Opera browser extension
Recommendation	Remove AllBlock browser extension from web browsers
CVE-ID	N/A

---

---

## Trickbot malware resurfaced

### Description

The infamous TrickBot malware has resurfaced that aims to expand the deployment of ransomware. The attackers responsible for performing malicious activities have been discovered to team up with other cybercrime gangs. TrickBot initially started from a banking trojan and now it is evolving to be a modular Windows-based crimeware solution.

Source	<a href="https://securityintelligence.com/posts/trickbot-gang-doubles-down-enterprise-infection/">https://securityintelligence.com/posts/trickbot-gang-doubles-down-enterprise-infection/</a>
Infected Technology	Windows
Recommendation	Monitor assets for any malicious activities, aware users regarding phishing
CVE-ID	N/A

---

---

## Latest Campaigns to steal OTP using Telegram Bots

---

### Description

A campaign where attackers are providing service to steal OTP tokens from the victims. The service is commenced via Telegram bots or offer customer support via Telegram channels. The bots automatically call targets as a part of phishing scam with the end goal to steal OTP codes. Attackers used SMS Buster to target eight Canadian-based banks.

Source	<a href="https://cyware.com/news/telegram-bots-used-in-latest-campaigns-to-steal-otps-bd401a98">https://cyware.com/news/telegram-bots-used-in-latest-campaigns-to-steal-otps-bd401a98</a>
--------	---

Infected Technology	Apache HTTP Server
---------------------	--------------------

Recommendation	Upgrade servers to Apache HTTP 2.4.51
----------------	---------------------------------------

CVE-ID	CVE-2021-41773 CVE-2021-42013
--------	----------------------------------

---

For any queries/recommendations:  
Contact us: [whois@cryptogen\*\*nepal\*\*.com](mailto:whois@cryptogen<b>nepal</b>.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/>