

# October 31, 2022

## INFOSEC WEEKLY

#MADE4SECURITY

- Google fixes seventh Chrome zero-day exploited in attacks this year
- ConnectWise fixes RCE bug exposing thousands of servers to attacks
- Hackers Actively Exploiting Cisco AnyConnect and GIGABYTE Drivers Vulnerabilities
- Apple iOS and macOS Flaw Could've Let Apps Eavesdrop on Your Conversations with Siri
- High-Severity Flaws in Juniper Junos OS Affect Enterprise Networking Devices



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.

---

## Google fixes seventh Chrome zero-day exploited in attacks this year

### Description

An emergency security update was released by google for the Chrome desktop web browser to address a single vulnerability known to be exploited in attacks. A type of confusion bug in Chrome V8 JavaScript engine. Access to bug details and links are kept restricted until most users are updated with fix. A type of confusion vulnerabilities occurs when the program allocates a resource, object, or variable using a type and then access it using a different, incompatible type, resulting in out-of-bounds memory access.

Source	<a href="https://www.bleepingcomputer.com/news/security/google-fixes-seventh-chrome-zero-day-exploited-in-attacks-this-year/">https://www.bleepingcomputer.com/news/security/google-fixes-seventh-chrome-zero-day-exploited-in-attacks-this-year/</a>
--------	---

Infected Technology	Google Chrome
---------------------	---------------

Recommendation	Update to latest version
----------------	--------------------------

CVE_ID	CVE-2022-3723
--------	---------------

---

---

## ConnectWise fixes RCE bug exposing thousands of servers to attacks

### Description

A security update has been released to address a critical vulnerability by the ConnectWise in the ConnectWise Recover and R1Soft Server Backup Manager (SBM) secure backup solutions. The security flaw is due to an injection weakness “Improper Neutralization of Special Elements in Output Used by a Downstream Component”. The vulnerability is detected as critical severity vulnerability that could enable attackers to access confidential data or execute code remotely. This vulnerability can also be used to push ransomware.

Source	<a href="https://www.bleepingcomputer.com/news/security/connectwise-fixes-rce-bug-exposing-thousands-of-servers-to-attacks/">https://www.bleepingcomputer.com/news/security/connectwise-fixes-rce-bug-exposing-thousands-of-servers-to-attacks/</a>
--------	---

Infected Technology	ConnectWise Recover SBMs
---------------------	--------------------------

Recommendation	Update to latest version
----------------	--------------------------

---

## Hackers Actively Exploiting Cisco AnyConnect and GIGABYTE Drivers Vulnerabilities

### Description

An active exploitation attempt targeting a pair of two-year-old security flaws in the Cisco AnyConnect Secure Mobility Client for Windows has been warned by Cisco. The vulnerabilities could enable local authenticated attackers to perform DLL hijacking a copy arbitrary file to system directories with elevated privileges. The vulnerability permits an attacker to escalate privileges and run malicious code to take complete control of an affected system. Gaining initial access is the exploitation of the above-stated Cisco AnyConnect flaws, with the GIGABYTE driver weakness employed to disarm security software.

Source	<a href="https://thehackernews.com/2022/10/hackers-actively-exploiting-cisco.html">https://thehackernews.com/2022/10/hackers-actively-exploiting-cisco.html</a>
--------	---

Infected Technology	Cisco AnyConnect and GIGABYTE Drivers
---------------------	---------------------------------------

Recommendation	Update to latest version
----------------	--------------------------

CVE_ID	CVE-2020-3153, CVE-2020-3433
--------	------------------------------

---

---

## Apple iOS and macOS Flaw Could've Let Apps Eavesdrop on Your Conversations with Siri

### Description

A security flaw in Apple's iOS and Mac operating systems might have allowed applications to listen in on Siri interactions. This would occur even if the app did not seek microphone access from Siri. Any app with Bluetooth access might have captured your Siri talks and audio from the iOS keyboard dictation capability while using AirPods or Beats headphones. The attack needs the app to have Bluetooth access, however, this restriction is easily bypassed. This is because customers are unlikely to anticipate that it will also allow them to access their Siri conversations and audio from dictation. On macOS, the vulnerability may be used to completely bypass the Transparency, Consent, and Control (TCC) security system, allowing any program to record Siri interactions without first obtaining permission

Source	<a href="https://thehackernews.com/2022/10/apple-ios-and-macos-flaw-couldve-let.html">https://thehackernews.com/2022/10/apple-ios-and-macos-flaw-couldve-let.html</a>
--------	---

Infected Technology	Apple's iOS and macOS
---------------------	-----------------------

Recommendation	Update to iOS 16.1.
----------------	---------------------

CVE_ID	CVE-2022-32946
--------	----------------

---

---

## High-Severity Flaws in Juniper Junos OS Affect Enterprise Networking Devices

### Description

A vulnerability in the Junos OS J-Web component can lead to arbitrary file write, resulting in remote code execution. An unauthenticated remote attacker can use this vulnerability to deserialize remote phar files. Other high-severity security issues affecting Juniper Networks devices have been revealed. A pre-authenticated reflected XSS on the error page ("error.php"), allowing a remote adversary to steal a Junos OS admin session and chain with other authentication-required issues. A remote authenticated attacker exploited two XPATH injection issues to obtain and alter Junos OS admin sessions. A path traversal weakness that might allow a remote authenticated attacker to upload PHP files to any arbitrary place, like the newly discovered RARlab UnRAR bug. A local file inclusion vulnerability might be used to run untrusted PHP code.

Source	<a href="https://thehackernews.com/2022/10/high-severity-flaws-in-juniper-junos-os.html">https://thehackernews.com/2022/10/high-severity-flaws-in-juniper-junos-os.html</a>
--------	---

Infected Technology	Juniper Junos OS
---------------------	------------------

Recommendation	Update latest software patch
----------------	------------------------------

CVE_ID	CVE-2022-22241, CVE-2022-22242, CVE-2022-22243, CVE-2022-22244, CVE-2022-22245, CVE-2022-22246
--------	--

---

For any queries/recommendations:  
Contact us: [whois@cryptogennepal.com](mailto: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/>