July 11, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Node.js fixes multiple bugs that could lead to RCE, HTTP request smuggling
- Hackers Exploiting Follina Bug to Deploy Rozena Backdoor
- Fortinet patch batch remedies multiple path traversal vulnerabilities
- Update Google Chrome Browser to Patch New Zero-Day Exploit Detected in the Wild
- Patch released for OpenSSL bug that could enable RCE

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.

Node.js fixes multiple bugs that could lead to RCE, HTTP request smuggling	
Description	
Node.js maintainers have released several solutions for JavaScript runtime environment vulnerabilities that might lead to arbitrary code execution and HTTP request smuggling, among other things. The specifics of seven now-patched issues, including three unique HTTP Request Smuggling vulnerabilities were revealed in an advisory Friday night (July 7). These three flaws - a defective parsing of transfer-encoding bug (CVE-2022-32213), an inappropriate delimiting of header fields issue (CVE-2022-32214), and an incorrect parsing of multi-line transfer-encoding bug (CVE-2022-32215) - might all lead to HTTP request smuggling.	
Source	https://portswigger.net/daily-swig/business-email-platform-zimbra-patches-memcached-injection-flaw-that-imperils-user-credential
Infected Technology	Versions of the 18.x, 16.x, and 14.x releases
Recommendation	Update to latest Patch version
CVE_ID	CVE-2022-32213, CVE-2022-32214, CVE-2022-3221

Hackers Exploiting Follina Bug to Deploy Rozena Backdoor	
Description	
A recently discovered phishing attempt is using the security hole known as Follina to spread an unauthorized backdoor on Windows computers. Backdoor virus called Rozena can inject a remote shell connection back to the attacker's computer. Word.exe, the Rozena implant, and cd.bat, a batch program created to stop MSDT processes, provide persistence to the backdoor by altering the Windows Registry, and download a normal Word document as a decoy. The main purpose of the virus is to inject shellcode that opens a reverse shell to the attacker's host ("microsofto.duckdns[.]org") and, in doing so, grants the attacker access to the system needed to monitor and collect data while also keeping a backdoor open to the compromised machine.	
Source	https://thehackernews.com/2022/07/hackers-exploiting-follina-bug-to.html
Infected Technology	Microsoft Excel, Windows shortcut (LNK), MS Word, Windows
Recommendation	Disable Office macros during downloading files

Fortinet patch batch remedies multiple path traversal vulnerabilities	
Description	
A raft of security vulnerabilities affecting several of its endpoint security products was addressed by Fortinet. A quartet of high severity flaws including multiple relative path transversal bugs in the management interface of FortiDeceptor, which spins up virtual machines that serve as honeypots for network intruders. Four high, six medium and one low severity issues were fixed by releasing a huge number of firmware and software updates on Tuesday (July 5). Abuse of such vulnerabilities may allow a remote and authenticated attacker to retrieve and delete arbitrary files from the underlying filesystem via specially crafted web requests. And other products such as VPN of FortiClient, FortiNAC network were affected with the vulnerabilities.	
Source	https://portswigger.net/daily-swig/fortinet-patch-batch-remedies-multiple-path-traversal-vulnerabilities
Infected Technology	Fortinet products
Recommendation	Update to latest version
CVE_ID	CVE-2022-30302, CVE-2021-41031, CVE-2022-26117, CVE-2021-43072, CVE-2022-26120, CVE-2022-27-483, CVE-2022-29057, CVE-2022-26118, CVE-2021-44170, CVE-2021-42755, CVE-2022-23438

Update Google Chrome Browser to Patch New Zero-Day Exploit Detected in the Wild	
Description	
Last Monday Google shipped security updates to address a high-severity zero-day vulnerability in its Chrome web browser that it said is being exploited in the wild. The shortcoming tracked as CVE-2022-2294, relates to a heap overflow flaw in the WebRTC component that provides real-time audio and video communication capabilities in browsers without the need to install plugins or download native apps. Heap buffer overflows, also referred to as heap overrun or heap smashing, occur when data is overwritten in the heap area of the memory, leading to arbitrary code execution or a denial-of-service (DoS) condition.	
Source	https://thehackernews.com/2022/07/update-google-chrome-browser-to-patch.html
Infected Technology	Linux Endpoints
Recommendation	Update to the latest version 103.0.5060.114 for Windows, macOS, and Linux and 103.0.5060.71 for Android.
CVE_ID	CVE-2022-2294

Patch released for OpenSSL bug that could enable RCE	
Description	
A serious flaw in the implementation of RSA in OpenSSL could enable attackers to perform remote code execution (RCE) due to a presence of a heap memory corruption vulnerability. According to the advisory “SSL/TLS servers or other servers using 2048-bit RSA private keys running on machines supporting AVX512IFMA instructions of the X84_64 architecture is affected by this issue.” The maintainers of the OpenSSL project have released patches to address this high-severity vulnerability.	
Source	https://thehackernews.com/2022/07/openssl-releases-patch-for-high.html
Infected Technology	OpenSSL version 3.0.4
Recommendation	Update to the version 3.0.5
CVE_ID	CVE-2022-2274

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/