October 4, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Two actively exploited 0-day vulnerability in Google Chrome
- New Azure AD Bug Lets Hackers Brute-Force Passwords Without Getting Caught.
- New malware targeting Active Directory FS servers
- Security Researcher from fortinet found multiple vulnerabilities on Corel products
- Implementation mistakes has high risk on Elastic Stack

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.

Two actively exploited 0-day vulnerability in Google Chrome

Description	
Google released urgent security fixes for its Chrome browser, including a pair of new security weaknesses that the company said are being exploited in the wild, making them the fourth and fifth actively zero-days plugged this month alone. The issues, designated as CVE-2021-37975 and CVE-2021-37976, are part of a total of four patches, and concern a use-after-free flaw in V8 JavaScript and WebAssembly engine as well as an information leak in core.	
Source	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_30.html
Infected Technology	Google Chrome
Recommendation	Update the security update released
CVE_ID	CVE-2021-37975, CVE-2021-37976

New Azure AD Bug Lets Hackers Brute-Force Passwords Without Getting Caught.

Description	
Cybersecurity researchers have disclosed an unpatched security vulnerability in the protocol used by Microsoft Azure Active Directory that potential adversaries could abuse to stage undetected brute-force attacks. This flaw allows threat actors to perform single-factor brute-force attacks against Azure Active Directory (Azure AD) without generating sign-in events in the targeted organization's tenant. The weakness resides in the Seamless Single Sign-On feature that allows employees to automatically sign when using their corporate devices that are connected to enterprise networks without having to enter any passwords.	
Source	https://www.secureworks.com/research/undetected-azure-active-directory-brute-force-attacks
Infected Technology	Azure AD
Recommendation	Update the latest available patch

New malware targeting Active Directory FS servers

Description	
Microsoft has revealed a new malware, codenamed FoggyWeb, targeting Active Directory Federation Services (AD FS) servers. The malware is being deployed by Nobelium hacking group behind SolarWinds supply chain attack to deliver additional payloads and steal sensitive information. The hacking group uses FoggyWeb to remotely exfiltrate the configuration database of compromised AD FS servers, decrypted token-signing certificate, and token-signing certificate, and token-decryption certificate, as well as to download and execute additional components.	
Source	https://www.microsoft.com/security/blog/2021/09/27/foggyweb-targeted-nobelium-malware-leads-to-persistent-backdoor/
Infected Technology	Microsoft Active Directory Federation Services
Recommendation	Review AD FS Server configuration

Security Researcher from fortinet found multiple vulnerabilities on Corel products

Description	
Fortinet's Security Researcher found in total of 15 zero-day vulnerabilities related to several Corel products. The list of vulnerabilities includes multiple Memory Corruption exploits. These attacks can cause unintended reads or information leak attack.	
Source	https://www.fortinet.com/blog/threat-research/fortinet-security-researcher-discovers-multiple-vulnerabilities-across-multiple-corel-products?&web_view=true
Infected Technology	Corel Products
Recommendation	Fortinet has advised to use caution when opening files from unknown sources and update Corel system right after patch releases.
CVE	CVE-2021-38096, CVE-2021-38097, CVE-2021-38098, CVE-2021-38099, CVE-2021-38100, CVE-2021-38101, CVE-2021-38102, CVE-2021-38103, CVE-2021-38104, CVE-2021-38105, CVE-2021-38106, CVE-2021-38107, CVE-2021-38108, CVE-2021-38109, CVE-2021-38110

Implementation mistakes has high risk on Elastic Stack

Description	
Cyber Security researchers from Salt Security discovered issues that enabled them to extract sensitive customer data. This also allowed any user to create a DOS condition that would make the system unavailable for the users. It was discovered that every customer using Elastic Stack itself.	
Source	https://www.zdnet.com/article/security-report-highlights-cybersecurity-dangers-of-elastic-stack-implementation-mistakes/?&web_view=true
Infected Technology	Elastic Stack
Recommendation	Use the Securing elastic stack guide for proper implementation
CVE-ID	N/A

Banking android malware named Flubot spreading via fake security updates

Description	
Researchers have found a high rise in Flubot malware which is proven more effective lure to compromise Android devices. The malware is trying to trick its victims into infecting themselves with the help of fake security updates warning them of Flubot infections. The malware is known to be delivered via SMS and phishing and tricking victims into giving additional permissions.	
Source	https://www.cert.govt.nz/individuals/news-and-events/parcel-delivery-text-message-infecting-android-phones/
Infected Technology	Android devices
Recommendation	Do not click on suspicious emails carried via text messages
CVE-ID	N/A

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/