July 18, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Hackers Targeting VoIP Servers by Exploiting Digium Phone Software
- Microsoft Teams security vulnerability left users open to XSS via flawed stickers feature
- Fantasy Premier League football app introduces 2FA to tackle account takeover hacks
- High severity OpenSSL bug could lead to remote code execution.

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.

Hackers Targeting VoIP Servers by Exploiting Digium Phone Software

Description	
A web shell was dropped on the servers of VoIP phones running Digium's software as part of an attack operation meant to exfiltrate data by downloading and running additional payloads. The virus downloads fresh payloads for execution installs multilayer obfuscated PHP backdoors into the file system of the web server, and plans repeating tasks to re-infect the host machine. The incursions resemble the INJ3CTOR3 campaign, which the Israeli cybersecurity company Check Point exposed in November 2020, suggesting that they may be a "resurgence" of earlier attacks. The attack begins with a remote server being used to retrieve the first dropper shell script, which is then used to install the PHP web shell in various areas throughout the file system and to create two root user accounts for further remote access. Additionally, a minutely running scheduled job is created that obtains a remote copy of the attacker-controlled domain's shell script for execution.	
Source	https://thehackernews.com/2022/07/hackers-targeting-voip-servers-by.html
Infected Technology	VoIP phones using Digium's software
Recommendation	• Update to the latest versions
CVE_ID	CVE-2021-45461

Microsoft Teams security vulnerability left users open to XSS via flawed stickers feature

Description	
The popular sticker features in Microsoft Teams could be abused to conduct cross-site scripting (XSS) attacks. The bug was discovered in the preview process of images sent via Teams to leak Skype tokens (PDF) and trigger an account takeover vulnerability in Teams iOS. When a sticker is sent via Teams, the platform converts it into an image and uploads the content as ‘RichText/HTML’ in the subsequent messages.	
Source	https://portswigger.net/daily-swig/microsoft-teams-security-vulnerability-left-users-open-to-xss-via-flawed-stickers-feature
Infected Technology	Microsoft Teams
Recommendation	Update to latest version
CVE_ID	CVE-2021-24114

High severity OpenSSL bug could lead to remote code execution.

Description

A high severity vulnerability in OpenSSL could allow a malicious actor to achieve remote code execution (RCE) on server-side devices. OpenSSL is a widely used cryptography library that provides an open-source implementation of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. It includes tools for generating RSA private keys and performing encryption and decryption, among other tasks. An alert indicates that the OpenSSL 3.0.4 version introduced a "severe problem" in the RSA implementation for X86 64 CPUs implementing the AVX512IFMA instructions. Because to this flaw, the RSA implementation with 2048-bit private keys is incorrect, resulting in memory corruption during the computation. An attacker may be able to cause RCE on the computer doing the computation because of the memory corruption, according to OpenSSL maintainers.

Source	https://portswigger.net/daily-swig/fantasy-premier-league-football-app-introduces-2fa-to-tackle-account-takeover-hacks
Infected Technology	OpenSSL 3.0.4 Version
Recommendation	OpenSSL 3.0.5. OpenSSL 1.1.1 and 1.0.2 are not affected by this issue.
CVE_ID	CVE-2022-2274

Fantasy Premier League football app introduces 2FA to tackle account takeover hacks

Description

The English Premier League (EPL) has added two-factor authentication (2FA) controls to its official Fantasy Premier League game (FPL), allowing football enthusiasts to safeguard their accounts. The introduction of 2FA for the 2022/23 season comes after a surge of account hijacking attack claims in the previous two seasons. Miscreants were reported to have conducted several 'transfers' of players from hacked accounts, leaving victims with poorer fantasy football teams while accruing penalty points. Victims battled to make up lost ground, and many had their entire season wrecked. The as-yet unnamed attackers, whose goals might vary from mischief to sabotage, were also in the practice of changing the team names of hacked victims.

Source	https://portswigger.net/daily-swig/fantasy-premier-league-football-app-introduces-2fa-to-tackle-account-takeover-hacks
Infected Technology	Fantasy Premier League football App
Recommendation	Upgrade to latest Patch
CVE_ID	-

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/