September 26, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Sophos Patches Actively Exploited Zero-Day Firewall Vulenrability
- Attackers Using Fake CircleCI Notifications to Hack GitHub Accounts
- QNAP Warns of OpenSSL Infinite Loop Vulnerability Affecting NAS Devices
- Microsoft Issues Out-of-Band Patch for Flaw Allowing Lateral Movement, Ransomware Attacks.
- Critical Magento vulnerability targeted in new surge of attacks

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.

Sophos Patches Actively Exploited Zero-Day Firewall Vulenrability

Description

The cybersecurity company, SOHPOS has released a patch for its firewall to remediate a zero-day flaw. This vulnerability was actively exploited by a Chinese APT (Advanced Persistent Threat) named DriftingCloud. According to the company, “this vulnerability being used to target a small set of specific organizations, primarily in the South Asia region”

Source	https://thehackernews.com/2022/09/hackers-actively-exploiting-new-sophos.html
Infected Technology	Sophos Firewall v19.0 MR1 (19.0.1) and older
Recommendation	Ensure that user portal is not exposed to WAN and update to the latest supported version • v19.5 GA • v19.0 MR2 (19.0.2) • v19.0 GA, MR1, and MR1-1 • v18.5 MR5 (18.5.5) • v18.5 GA, MR1, MR1-1, MR2, MR3, and MR4 • v18.0 MR3, MR4, MR5, and MR6 • v17.5 MR12, MR13, MR14, MR15, MR16, and MR17 • v17.0 MR10
CVE_ID	CVE-3236

Attackers Using Fake CircleCI Notifications to Hack GitHub Accounts

Description

GitHub has issued an advice outlining what appears to be an ongoing phishing campaign aimed at stealing passwords and two-factor authentication (2FA) codes by mimicking the CircleCI DevOps platform. The attack was discovered on September 16, 2022, according to the Microsoft-owned code hosting service, and it damaged "several victim businesses." The fake messages pretend to inform users that their CircleCI sessions have expired and that they should check in with their GitHub credentials by clicking on a link. If the hijacked account has organization management access, the attacker has also been seen stealing private repository contents and establishing and adding new GitHub accounts to an organization. GitHub stated that it has reset passwords and removed maliciously-added credentials for impacted users, as well as notified those affected and suspended the actor-controlled accounts.

Source	https://thehackernews.com/2022/09/hackers-using-fake-circleci.html
Infected Technology	Github User Accounts
Recommendation	Stay up to date with Security news related to Github

QNAP Warns of OpenSSL Infinite Loop Vulnerability Affecting NAS Devices

Description

A vulnerability in Netlify could allow an attacker to achieve either persistent cross-site scripting (XSS) or full-response server-side request forgery on any supported website. By submitting specially constructed headers, an attacker might get around the source image domain allow list and get the handler to load and deliver random pictures. The picture would subsequently be delivered to visitors without requiring those headers to be specified. A malicious SVG file with embedded scripts might therefore be requested by an attacker and subsequently provided from the site domain, resulting in XSS.

Source	https://portswigger.net/daily-swig/netlify-vulnerable-to-xss-ssrf-attacks-via-cache-poisoning
Infected Technology	Netlify (NAS Devices)
Recommendation	Update to version 1.2.3
CVE_ID	CVE-2022-39239

Microsoft Issues Out-of-Band Patch for Flaw Allowing Lateral Movement, Ransomware Attacks.

Description	
Microsoft this week released an out-of-band security update for its Endpoint Configuration Manager solution to patch a vulnerability that could be useful to malicious actors for moving around in a targeted organization's network. The vulnerability is tracked as CVE-2022-37972 and it has been described by Microsoft as a medium-severity spoofing issue. In its advisory, Microsoft said there is no evidence of exploitation, but the vulnerability has been publicly disclosed. Microsoft Endpoint Configuration Manager (MECM), an on-premises management solution for desktops, servers and laptops, allowing users to deploy updates, apps, and operating systems. One method for deploying the needed client application to endpoints is client push installation, which enables admins to easily and automatically push clients to new devices. The MECM vulnerability patched this week by Microsoft with an out-of-band update is related to the use of NTLM authentication.	
Source	https://www.securityweek.com/microsoft-issues-out-band-patch-flaw-allowing-lateral-movement-ransomware-attacks
Infected Technology	Microsoft Endpoint Configuration Manager (MECM)
Recommendation	Update to the latest version.
CVE_ID	CVE-2022-37972

Critical Magento vulnerability targeted in new surge of attacks

Description

A critical Magento vulnerability allowing unauthenticated attackers to execute code on unpatched sites was observed by researchers. Three attack variants exploit the vulnerability endpoints to inject a remote access trojan (RAT). The first variants begin with creating a new customer account on the target platform using template code in the first and last names. The injected code decodes to a command that downloads a Linux executable which launches in the background as a process. The attack involves the injection of a PHP backdoor by including template code in the VAT field of the placed order. The third attack variation employs template code that executes to replace "generated/code/Magento/Framework/App/FrontController/Interceptor.php" with a malicious, backdoored version.

Source	https://www.bleepingcomputer.com/news/security/critical-magento-vulnerability-targeted-in-new-surge-of-attacks/
Infected Technology	Magento
Recommendation	• Follow the security guidelines on support page • Update to latest version
CVE_ID	CVE-2022-24086

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/