April 25, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- XSS vulnerability in open-source tool Private Bin.
- Vulnerability in AWS Log4Shell Hot Patch Allowed Full Host Takeover
- A Bug That Could Paralyze Snort Intrusion Detection System
- Hackers can access emails due to unpatched bug in Rainloop
- POC released for a recent Java Cryptographic vulnerability

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.

XSS vulnerability in open-source tool Private Bin.

Description	
PrivateBin, the open source secure pastebin, has been patched to address a cross-site scripting (XSS) vulnerability. PrivateBin, a derivative of the famous ZeroBin, is an online application for storing data that is encrypted/decrypted in the browser using 256 bits AES, implying that the server has "zero knowledge of copied contents. "The bug, discovered by the researchers allows malicious JavaScript code to be placed in an SVG picture file, which may then be appended to pastes. An attacker can execute code if a user opens a paste with a specially designed SVG attachment and interacts with the preview picture when the instance is not protected by a proper content security policy.	
Source	https://portswigger.net/daily-swig/xss-vulnerability-in-open-source-tool-privatebin-patched
Infected Technology	Outdated Pastebin Version
Recommendation	• Upgrade to the latest patched version • Ensure the CSP of their instance is set correctly

Vulnerability in AWS Log4Shell Hot Patch Allowed Full Host Takeover

Description	
Patches designed to safeguard containers Amazon Web Services (AWS) containers that were vulnerable to the severe Log4Shell issue included major flaws that might allow rogue containers to compromise the underlying host. AWS launched "hot patch" services that operate on servers and detect and fix unpatched Java apps and containers on the fly due to the severity of Log4Shell.The updates are applicable to single servers, Kubernetes clusters, and Elastic Container Service (ECS) clusters. These updates can be implemented in other cloud environments or on standalone systems in addition to AWS. According to their results, every container in a cluster may use the vulnerability to escape and gain privileges. Unprivileged processes, in addition to containers, can use the patch service to escalate privileges and acquire root code execution.	
Source	https://portswigger.net/daily-swig/xss-vulnerability-in-open-source-tool-privatebin-patched
Infected Technology	Outdated AWS Version
Recommendation	Upgrade to the latest patched version

A Bug That Could Paralyze Snort Intrusion Detection System

Description	
Details have surfaced concerning a now-patched security flaw in the Snort intrusion detection and prevention system, which could cause a denial-of-service (DoS) scenario and make it helpless against malicious traffic. The vulnerability, identified as CVE-2022-20685, has a severity rating of 7.5 and is in the Snort detection engine's Modbus preprocessor. The vulnerability, CVE-2022-20685, is an integer-overflow flaw that can enable the Snort Modbus OT preprocessor to enter an indefinite while loop, said security researchers, in a paper released last week. "A successful hack prevents Snort from processing new packets and alerting."	
Source	https://portswigger.net/daily-swig/xss-vulnerability-in-open-source-tool-privatebin-patched
Infected Technology	Snort open-source project releases prior to version 2.9.19 and 3.1.11.0.
Recommendation	Upgrade to the latest version
CVE_ID	CVE-2022-20685

POC released for a recent Java Cryptographic vulnerability

Description	
Security researcher, Khaled Nassar released a Proof of Concept (POC) for a cryptographic vulnerability that if successfully exploited, could enable attackers to forge signatures and bypass authentication measures. The security weakness (dubbed Psychic Signatures) makes it possible for an attacker to present a blank signature which is accepted as valid. This makes it trivial for an attacker to bypass ECDSA signatures for security mechanism if the server is running Java version 15,16,17 or 18.	
Source	https://thehackernews.com/2022/04/researcher-releases-poc-for-recent-java.html
Infected Technology	• Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18 • Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1, 22.0.0.2
Recommendation	Patch the vulnerability to mitigate exploit attempts.
CVE_ID	CVE-2022-21449

Hackers can access emails due to unpatched bug in Rainloop

Description	
A high-servility unpatched flaw in RainLoop web-based email client was disclosed that can enable threat actors to siphon emails from victim's inboxes. According to security researcher Simon Scannell, the vulnerability can be easily exploited by an attacker by sending a specially crafted email to a victim that uses Rain Loop. When the victim views the email, the attacker can gain full control over the session and steal any email. Sonar Source reported the vulnerability on November 30,2021 but the vendor has failed to provide a patch for more than four months.	
Source	https://thehackernews.com/2022/04/unpatched-bug-in-rainloop-webmail-could.html
Infected Technology	RainLoop version 1.16.0
Recommendation	• Do not open email from unknown sources. • Migrate to SnappyMail (a RainLoop Fork)
CVE_ID	CVE-2022-29360

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/