InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Vulnerability Found in Linux's Sudo' command
2. Privilege escalation on solaris
3. VMware Patches critical bug in Harbor Container
4. Cisco critical Aironet Access Points Flaw
5. Kubernetes Bugs Allow Authentication Bypass, DoS

20/10/2019

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.

1. Vulnerabilty found in linux's 'sudo' command

Description	
A new vulnerability in Sudo -core command that is installed on almost every UNIX and Linux-based operating system- was discovered which could allow a malicious user or a program to execute arbitrary commands as root on a targeted Linux system even the "sudoers configuration" explicitly disallows the root access. This vulnerability could allow other users except root to bypass the security policy and take complete control over system as root. This flaw can be exploited by an attacker to run commands as root just by specifying the user id "-1" or "4294967295".	
Source	https://thehackernews.com/2019/10/linux-sudo-run-as-root-flaw.html
Infected Technology	Linux OS
Recommendation	Update sudo package to latest version when available
CVE_ID	CVE-2019-14287

2. Privilege escalation on Solaris 11

Description	
Exploitation of a design vulnerability in Xscreensaver, as distributed with Solaris 11.x allows attackers to create arbitrary files on the system, by abusing the -log command line switch introduced in version 5.06. This flaw can be leveraged to cause a Denial of Service (DoS) condition or to escalate privileges to root. This vulnerability in Solaris is caused by the fact that Oracle maintains a slightly different codebase from the upstream one.	
Source	https://techblog.mediaservice.net/2019/10/local-privilege-escalation-on-solaris-11-x-via-xscreensaver/
Infected Technology	Oracle Solaris
Recommendation	Update patch when available
CVE_ID	CVE-2019-3010

3. VMware patches critical bug in Harbor Container Registry for PCF

Description	
A critical "broken access control" vulnerability found in VMware Cloud Foundation and Harbor Container Registry for Pivotal Cloud Foundry. This vulnerability let malicious actors with administrative access which could potentially exploit the flaw in order to "create a robot account inside of an adjacent project via the Harbor API". Doing so would allow them to push, pull or modify images in the targeted adjacent project.	
Source	https://www.scmagazine.com/home/network-security/vmware-patches-critical-bug-in-harbor-container-registry-for-pcf/
Infected Technology	VMware
CVE_ID	CVE-2019-16919

4. Cisco Critical Aironet points flaw

Description	
A critical unauthorized access bug was found in the company's Cisco Aironet Access Points (APs) software which could be potentially exploited to view sensitive information, interfere with configuration options and disable the AP, in order to create a denial of service condition for clients associated with AP. An attacker could exploit this vulnerability by requesting specific URLs from an affected AP. This exploit could allow an attacker to gain access to the device with elevated privileges.	
Source	https://www.scmagazine.com/home/network-security/cisco-fixes-critical-aironet-access-points-flaw-addresses-29-more-bugs/
Infected Technology	Cisco Aironet Series
Recommendation	Update the released patch
CVE_ID	CVE-2019-15260

5. Kubernetes Bugs Allow Authentication Bypass,DoS

Description	
The kubernetes API server can be used for authentication and access control to identify users through request headers.This issue arises because in the HTTP specification, no whitespace is allowed in the request header due to which the proxy could ignore invalid headers and forward them to the GO server which would interpret these headers as valid. So attackers could exploit the bug to authenticate as any user by crafting an invalid header that would go through the server. The kubernetes API server is also vulnerable to denial of service (DoS) that can be aimed at the YAML/JSON parsing function. Kubernetes API server allows authorized users to send malicious YAML or JSON payloads, causing the API server to consume excessive CPU or memory, potentially crashing and becoming unavailable.	
Source	https://threatpost.com/kubernetes-bugs-authentication-bypass-dos/149265/
Infected Industry	Kubernetes
Recommendation	Patch immediately when available
CVE ID	CVE-2019-16276 , CVE-2019-11253

For any queries/recommendations:

Contact us: **whois@cryptogennepal.com**