May 9, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Google Releases Android Update to Patch Actively Exploited Vulnerability
- F5 warns of critical BIG-IP RCE bug allowing device takeover.
- TLStorm 2.0 Bugs Affect Aruba and Avaya Network Switches
- Root access to NFVIS hosts
- QNAP Releases Firmware Patches for 9 New Flaws Affecting NAS Devices

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.

Google Releases Android Update to Patch Actively Exploited Vulnerability

Description	
Google has released monthly security patches for Android with fixes for 37 flaws across different components, one of which is a fix for an actively exploited Linux kernel vulnerability that came to light earlier this year. Tracked as (CVSS score: 7.8), the vulnerability is ranked "High" for severity and could be exploited by a local user to escalate privileges or deny service. The issue relates to a double-free vulnerability residing in the Packet network protocol implementation in the Linux kernel that could cause memory corruption, potentially leading to denial-of-service or execution of arbitrary code.	
Source	https://thehackernews.com/2022/05/google-releases-android-update-to-patch.html
Infected Technology	Android Technology
Recommendation	Update the patch released.
CVE_ID	CVE-2021-22600

F5 warns of critical BIG-IP RCE bug allowing device takeover.

Description	
A security advisory warning about the flaw which may allow unauthenticated attackers with network access to execute arbitrary system command, perform file actions, and disable services on BIG-IP was issued by F5 on its various versions ranging from 11 to 16. The detected flaws lie in the iControl REST component and allows a malicious actor to send undisclosed requests to bypass the iControl REST authentication in BIG-IP.	
Source	https://www.bleepingcomputer.com/news/security/f5-warns-of-critical-big-ip-rce-bug-allowing-device-takeover/
Infected Technology	BIG-IP version 11.6.1 to 11.6.5, 12.1.0 to 12.1.6, 13.1.0 to 13.1.4, 14.1.0 to 14.1.4, 15.1.0 to 15.1.5 and 16.1.0 to 16.1.2
Recommendation	• Update to latest version
CVE_ID	CVE-2022-13388

TLStorm 2.0 Bugs Affect Aruba and Avaya Network Switches

Description	
Researchers have discovered up to five serious security weaknesses in the implementation of the TLS protocol in certain models of Aruba and Avaya network switches, which might be exploited to obtain remote access to company networks and steal sensitive data. APC Smart-UPS systems have three serious weaknesses that might allow an attacker to gain control and, worse, physically destroy the units. IoT security firm Armis discovered, which pointed to a similar source: a misuse of NanoSSL, a standards-based SSL developer suite from Mocana, a DigiCert affiliate. Vulnerabilities found in Avaya switches are zero-click, meaning they can be activated via unauthenticated network packets without any user interaction. This means that network segmentation alone is no longer sufficient as a security measure to protect against cyber-attacks, according to researchers.	
Source	https://thehackernews.com/2022/05/critical-tlstorm-20-bugs-affect-widely.html
Infected Technology	Avaya ERS3500 Series, ERS3600 Series, ERS4900 Series, ERS5900 Series, Aruba 5400R Series, 3810 Series, 2920 Series, 2930F Series, 2930M Series, 2530 Series, 2540 Series
Recommendation	Update to the latest version.
CVE_ID	CVE-2022-23676, CVE-2022-23677, CVE-2022-29860, CVE-2022-29861

Root access to NFVIS hosts	
Description	
An attacker could take advantage of this flaw by submitting an API call from a VM running on the NFVIS host with root access. An attacker could completely compromise the NFVIS host if the exploit is successful. Cisco Enterprise NFVIS' Next Generation Input/Output (NGIO) functionality contained one of the security weaknesses, a critical guest escape dubbed CVE-2022-20777. Insufficient guest limitations cause CVE-2022-20777, which allows authenticated attackers to leave the guest VM and acquire root-level access to the host without requiring user input in low-complexity attacks. A second vulnerability (CVE-2022-20779) is a high severity command injection vulnerability in Cisco Enterprise NFVIS' image registration procedure due to insufficient input validation. An attacker could take advantage of this flaw by convincing a host system administrator to install a VM image with specially designed metadata that will run commands with root privileges during the VM registration process. A successful exploit could allow the attacker to insert commands into the NFVIS host with root-level privileges.	
Source	https://www.bleepingcomputer.com/news/security/cisco-fixes-nfvis-bugs-that-help-gain-root-and-hijack-hosts/
Infected Technology	NFVIS guest VM, Image Registration in NFVIS
Recommendation	Update to latest version of NFVIS
CVE_ID	CVE-2022-20777, CVE-2022-20779

QNAP Releases Firmware Patches for 9 New Flaws Affecting NAS Devices

Description	
QNAP, a Taiwanese manufacturer of network-attached storage (NAS) devices, released security upgrades on Friday to address nine security flaws, including a serious vulnerability that could be used to take control of an affected system. In an advisory, QNAP stated that "a vulnerability has been reported to harm QNAP VS Series NVRs running QVR." "This vulnerability allows remote attackers to run arbitrary commands if exploited."	
Source	https://thehackernews.com/2022/05/qnap-releases-firmware-patches-for-9.html
Infected Technology	QNAP devices, NVR Devices
Recommendation	• Update to latest version
CVE_ID	CVE-2021-44051, CVE-2021-44052

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