February 28, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Link following vulnerability on Samba
- Cisco fixes critical bugs in Nexus Series Switches
- VMware Issues Security Patches for High-Severity Flaws
- Zero-day XSS vulnerability in horde webmail client
- Cisco FXOS and NX-OS Software Security Advisory Bundled Publication
- Critical Zabbix Vulnerability Exploited

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.

Link following vulnerability on Samba

Description	
Versions prior to 4.15.5 of Samba was determined to have a link following vulnerability. This vulnerability allows attackers to define if a file or directory exists but has no ability to access these files or directories in an area of the server file system via symlink. This vulnerability was assigned the CVE-2021-44141 with the CVSS 3.5 base score of 4.2.	
Source	https://cyber.vumetric.com/vulns/CVE-2021-44141/link-following-vulnerability-in-multiple-products/
Infected Technology	Samba prior to 4.15.5
Recommendation	Upgrade to the latest samba version
CVE_ID	CVE-2021-44141

Cisco fixes critical bugs in Nexus Series Switches

Description	
Cisco has patched four critical security flaws in its Nexus Series switches that may be exploited by malicious actors to gain system control. An attacker sends a specially crafted HTTP POST request to the targeted device's NX-API. If the exploit is successful, the attacker will have root access on the underlying operating system and will be able to run arbitrary commands. Two high-severity denial-of-service (DoS) issues in Cisco Fabric Services Over IP have also been fixed. It did not, however, go into detail about the risk actors who may be misusing them.	
Source	https://thehackernews.com/2022/02/new-flaws-discovered-in-ciscos-network.html
Infected Technology	Nexus Series Switches like Nexus 3000, Nexus 5500, Nexus 5600, Nexus 6000 and Nexus 9000 Software that have the NX-API feature enabled.
Recommendation	Upgrade to the firmware to latest Version
CVE_ID	CVE-2022-20650 CVE-2022-20624 CVE-2022-20625 CVE-2022-20623

VMware Issues Security Patches for High-Severity Flaws

Description	
On Tuesday, 15 February, 2022 Vmware Patched several high-severity vulnerabilities impacting ESXi, Workstation, Fusion, Cloud Foundation, and NSX Data Center for vSphere that could be exploited to execute arbitrary code and cause a denial-of-service (DoS) condition. As of now, no weakness is exploited but malicious actor with local administrative access on a virtual machine might use the weaknesses to execute code as the virtual machine's VMX process running on the host.	
Source	https://thehackernews.com/2022/02/vmware-issues-security-patches-for-high.html
Infected Technology	VMware ESXi VMware Workstation Pro/ Player (Workstation) VMware Fusion Pro / Fusion (Fusion) VMware Cloud Foundation (Cloud Foundation)
Recommendation	Update Security Patch of the infected technology
CVE_ID	CVE-2021-22040 (CVSS score: 8.4) CVE-2021-22041 (CVSS score: 8.4) CVE-2021-22042 (CVSS score: 8.2) CVE-2021-22043 (CVSS score: 8.2) CVE-2021-22050 (CVSS score: 5.3) CVE-2022-22945 (CVSS score: 8.8)

Zero-day XSS vulnerability in horde webmail client

Description	
Security researchers from Sonar Source uncovered a cross-site scripting (XSS) vulnerability in Horde webmail client. Hord webmail client, by the horde project, is a popular open-source email service used by many universities and governments. Successful exploitation of this vulnerability enables attackers to steal user emails. The stored XSS vulnerability is caused by process of rendering OpenOffice files into viewable format using XSLT (eXtensible Stylesheet Language Transformations). This process is performed without adquicate sanitization leading to javascript code injection.	
Source	https://blog.sonarsource.com/horde-webmail-account-takeover-via-email
Infected Technology	Horde webmail client
Recommendation	At the time of writing, no official patches have been released by the vendor.

Cisco FXOS and NX-OS Software Security Advisory Bundled Publication

Description	
Cisco has released fixes for four vulnerabilities in its FXOS and NX-OS network operating systems. Three of the security issues are rated high severity; the fourth is rated medium. Cisco was alerted to one of the vulnerabilities – a fabric services over IP denial-of-service issue – by the National Security Agency (NSA). The fixes are part of Cisco's semi-annual FXOS and NX-OS Software Security Advisory Bundled Publication. The fixes include addressing CVE-2022-20650, which can be remotely exploited and allow command injection. The flaw identified by the NSA is CVE-2022-20624, resulting from insufficient validation of network packets, allowing specially crafted packets to exploit it.	
Source	https://www.securityweek.com/nsa-informs-cisco-vulnerability-exposing-nexus-switches-dos-attacks
Infected Technology	Cisco Nexus 9000 Series Switches
Recommendation	Update the firmware to latest version.

Critical Zabbix Vulnerability Exploited

Description	
If the instances are explicitly configured to allow SSO authentication via SAML, the malicious attacker can modify the session data as the session stored for user login is not verified properly. This lead to authentication bypass and even instance takeover via Zabbix Frontend with configured SAML caused by insecure client-side session storage.	
Source	https://support.zabbix.com/browse/ZBX-20350
Infected Technology	Zabbix 5.4.0 - 5.4.8 Zabbix 6.0.0alpha1
Recommendation	Disable the SAML SSO authentication till the fix releases
CVE_ID	CVE-2022-23131

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/