June 28
2021

INFOSEC WEEKLY

#MADE4SECURITY

- Unpatched Flaw in Linux Pling Store Apps Could Lead to Supply-Chain Attacks
- VMware Patches Privilege Escalation Vulnerability in Tools for Windows
- VMware Patches Critical Vulnerability in Carbon Black App Control
- Vulnerabilities Expose Fortinet Firewalls to Remote Attacks
- BIOS Disconnect: New High-Severity Bugs Affect 128 Dell PC and Tablet Models
- SonicWall Left a VPN Flaw Partially Unpatched Amidst 0-Day 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.

1. **Unpatched Flaw in Linux Pling Store Apps Could Lead to Supply-Chain Attacks**	
Description	
Cybersecurity researchers have disclosed a critical unpatched vulnerability affecting the Pling-based free and open-source software (FOSS) marketplace for the Linux platform that could be potentially abused to stage supply-chain attacks and achieve remote code execution (RCE). The vulnerability stems from the manner the store's product listings page parses HTML or embedded media fields, thereby potentially allowing an attacker to inject malicious JavaScript code that could result in arbitrary code execution. This stored XSS could be used to modify active listings or post new listings on the Pling store in the context of other users, resulting in a wormable XSS.	
Source	https://positive.security/blog/hacking-linux-marketplaces
Infected Technology	Pling-based apps
Recommendation	Install the latest security patch as soon as possible.

2. **VMware Patches Privilege Escalation Vulnerability in Tools for Windows**	
Description	
A high-severity vulnerability that VMware patched this week in VMware Tools for Windows could be exploited to execute arbitrary code with elevated privileges. The issue is a local privilege escalation that requires an attacker to have normal access to a virtual machine for successful exploitation. An attacker with normal access to a virtual machine may exploit this issue by placing a malicious file renamed as 'openssl.cnf' in an unrestricted directory which would allow code to be executed with elevated privileges.	
Source	https://www.vmware.com/security/advisories/VMSA-2021-0013.html
Infected Technology	• VMware Tools for Windows • VMware Remote Console (VMRC) for Windows • VMware App Volumes
CVE-ID	CVE-2021-21999
Recommendation	Consider updating to the latest patched version i.e., VMware Tools for Windows 11.2.6, VMRC for Windows 12.0.1, and App Volumes 4 release 2103/App Volumes 2.18

3. VMware Patches Critical Vulnerability in Carbon Black App Control

Description	
VMware this week announced the availability of patches for an authentication bypass vulnerability in VMware Carbon Black App Control (AppC) running on Windows machines. The newly addressed security hole, the company says, could be exploited by an attacker to gain unauthenticated administrative access to the application. According to VMware, even if the attacker doesn't need valid credentials for the target application, they would still have to first gain network access to the VMware Carbon Black App Control management server for the attack to succeed.	
Source	https://www.vmware.com/security/advisories/VMSA-2021-0012.html
Infected Technology	VMware Carbon Black App Control (AppC)
CVE ID	CVE-2021-21998
Recommendation	Consider applying the security patches released by VMware.

4. Vulnerabilities Expose Fortinet Firewalls to Remote Attacks

Description	
A high-severity vulnerability patched recently by Fortinet in its FortiWeb web application firewall (WAF) can be exploited to execute arbitrary commands. The flaw can pose an even more serious risk if it's chained with a misconfiguration and another recently discovered security hole It was found that the FortiWeb firewall — specifically its management interface — is affected by a vulnerability that can allow a remote, authenticated attacker to execute commands on the system via the SAML server configuration page. The researcher noted that the impact of the vulnerability can be even more serious if it's chained with a misconfiguration and a separate vulnerability.	
Source	https://www.fortiguard.com/psirt/FG-IR-20-120
Infected Technology	FortiWeb versions < 6.3.8 and 6.3.4
CVE ID	CVE-2021-22123
Recommendation	Consider updating FortiWeb to its latest version.

5. **BIOS Disconnect: New High-Severity Bugs Affect 128 Dell PC and Tablet Models**	
Description	
Cybersecurity researchers on Thursday disclosed a chain of vulnerabilities affecting the BIOSConnect feature within Dell Client BIOS that could be abused by a privileged network adversary to gain arbitrary code execution at the BIOS/UEFI level of the affected device. As the attacker has the ability to remotely execute code in the pre-boot environment, this can be used to subvert the operating system and undermine fundamental trust in the device. Successful exploitation of the flaws could mean loss of device integrity, what with the attacker capable of remotely executing malicious code in the pre-boot environment that could alter the initial state of the operating system and break OS-level security protections.	
Source	https://eclypsium.com/2021/06/24/biosdisconnect/
Infected Technology	128 Dell PC and Tablet Models
CVE ID	CVE-2021-21571, CVE-2021-21572, CVE-2021-21573 CVE-2021-21574
Recommendation	Consider installing the BIOS firm update released by Dell.

6. SonicWall Left a VPN Flaw Partially Unpatched Amidst 0-Day Attacks

Description	
A critical vulnerability in SonicWall VPN appliances that was believed to have been patched last year has been now found to be "botched," with the company leaving a memory leak flaw unaddressed, until now, that could permit a remote attacker to gain access to sensitive information. It's worth noting that SonicWall's decision to hold back the patch comes amid multiple zero day disclosures affecting its remote access VPN and email security products that have been exploited in a series of in-the-wild attacks to deploy backdoors and a new strain of ransomware called FIVEHANDS. However, there is no evidence that the flaw is being exploited in the wild.	
Source	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0006
Infected Technology	SonicWall VPN Appliences
CVE ID	CVE-2021-20019

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/