November 30, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- Phishing lures employees with fake 'back to work' internal memos
- Passwords of vulnerable Fortinet VPNs exposed
- VMware unpatched critical flaw
- Sophos security breach
- Office 365 phishing abusing Oracle and Amazon cloud services
- cPanel 2FA bypassed
- Drupal issues emergency fix for critical bug with known exploits

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. Phishing lures employees with fake 'back to work' internal memos

Description
Scammers are circulating a phishing email camouflaged as internal 'back-to-work' company memo. The phishing email have landed in thousands of mailboxes bypassing G suite email defense. The delivered emails are spoofed victim's company mail service with attached voicemails and HTML attachment with employee's name which redirects target to landing page requiring email address and password. The report has been provided by researchers at Abnormal Security, email security company.

Source	https://www.bleepingcomputer.com/news/security/phishing-lures-employees-with-fake-back-to-work-internal-memos/
Infected Technology	Phishing
Recommendation	Do not open attachment from unknown senders Do not provide credentials without verification of the logged in domain

2. Passwords of vulnerable Fortinet VPNs exposed

Description
A attack vector has released a list of targets vulnerable for CVE-2018-13379. The critical FortiOS vulnerability allows attacker access to sensitive files from Fortinet VPNs containing session related information which may reveal plain text username and passwords of Fortinet VPN users. Threat analysts have also found threads in hacker forum where dump files for vulnerable IPs has been shared. The dumps include username, passwords, access levels and original unmasked IP address of users connected to VPNs. Fortinet has reportedly requested customers to apply the patch released earlier.

Source	https://www.bleepingcomputer.com/news/security/passwords-exposed-for-almost-50-000-vulnerable-fortinet-vpns/
Infected Technology	Fortinet VPN
CVE	CVE-2018-13379
Recommendation	Update the patch released by OEM

3. VMware unpatched critical flaw

Description	
VMware has a critical vulnerability in its products that allows a perpetrator to execute commands with unrestricted privileges on the underlying OS. With network access to the admin configurator on port 8443 and a valid password for the admin account, the attacker can exploit and take control of the affected system.	
Source	https://thehackernews.com/2020/11/critical-unpatched-vmware-flaw-affects.html
Infected Technology	• VMware Workspace One Access v 20.01 | 20.10 (Linux and Windows) • VMware Workspace One Access Connector (v 20.10 | 20.01.0.0 | 20.01.0.1 (Windows) • VMware Identity Manager v 3.3.1 | 3.3.2 | 3.3.3 (Linux and Windows) • VMware Identity Manager Connector v 3.3.1 | 3.3.2 (Linux) v 3.3.1 | 3.3.2 | 3.3.3 (Windows) • VMware Cloud Foundation v 4.x (Linux and Windows) • vRealize Suite Lifecycle Manager v 8.x (Linux and Windows)
CVE	CVE-2020-4006
Recommendation	Follow the Solution given in the following link https://kb.vmware.com/s/article/81731

4. Sophos security breach

Description	
Sophos, a British cybersecurity and hardware company had their customers' personal information exposed due to a misconfigured tool used for storing customer information. The access permission issue led to the exposure of the information of a small number of customers who reached out to the company's support team. The data included the first and last names, email addresses and contact phone numbers of the users had they provided said information to the Sophos support.	
Source	https://www.arnnet.com.au/article/684762/sophos-customer-data-exposed-by-leak/

5. Office 365 phishing abusing Oracle and Amazon cloud services

Description	
Phishing campaign scheme for stealing office 365 credentials utilizes Oracle and Amazon web services as infrastructure. The campaign uses network of compromised legitimate websites. Although heavily dependent upon lure, the use of legitimate services and websites makes the campaign sophisticated. The threat actor sends phishing messages from compromised email account to lure victims to the compromised website. The compromised websites are suggested to be part of the phishing as a service business rented to various clients.	
Source	https://www.bleepingcomputer.com/news/security/office-365-phishing-abuses-oracle-and-amazon-cloud-services/
Infected Technology	Phishing
Recommendation	Do not open emails from unknown sources Enable 2FA on login credentials

6. cPanel 2FA bypassed

Description	
cPanel, webhosting control panel's security flaw allows malicious actors with knowledge of or access to valid credentials to work around a two-factor-authentication check with brute-force attacks for domains that are managed using the vulnerable cPanel & WebHost Manager (WHM) versions. Over 70 million domains are supposedly affected.	
Source	https://www.bleepingcomputer.com/news/security/cpanel-2fa-bypassed-in-minutes-via-brute-force-attacks/
Infected Technology	cPanel & WebHost Manager (WHM)
CVE	CVE-2020-27641
Recommendation	Security updates for the security flaw have been released for cPanel and WHM versions 11.92.0.2, 11.90.0.17, and 11.86.0.32, and are available for download through Software Update.

7. Drupal issues emergency fix for critical bug with known exploits

Description	
Drupal has released an emergency security updates to address critical vulnerability. The flaw could allow arbitrary code execution on some CMS version. Over 944,000 websites are affected by the vulnerability. The vulnerability is caused by two bugs which can be exploited when file uploads of compressed files is allowed. Drupal has released patched version for version above 7. Drupal has requested developers to block file uploads from untrusted user while the update is not available.	
Source	https://www.drupal.org/sa-core-2020-013
Infected Technology	Drupal
CVE	CVE-2020-28949, CVE-2020-28948
Recommendation	• Update to Drupal 9.0.9 for Drupal 9.0 • Update to Drupal 8.9.10 for 8.9 • Update to Drupal 8.8.12 for Drupal 8.8 or earlier • Update to Drupal 7.75 for Drupal 7

For any queries/recommendations:

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