InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Drupal 8 File Upload Vulnerability
2. LifeLabs Suffers Data Breach
3. This Bug Could Have Let Anyone Crash WhatsApp Of All Group Members
4. PayPal Phishing Attack Promises to Secure Accounts, Steals Everything
5. Remote Code Execution via Insecure Deserialization in Telerik UI

23/12/2019

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. Drupal 8 File Upload Vulnerability

Description	
A new vulnerability in Drupal 8 has been identified as it allows authenticated administrative users to upload a .htaccessfile that can modify the server's executable file extensions to achieve remote code execution. Under certain configurations, this vulnerability can be exploited by non-administrative users as well. This vulnerability was found in fiile_Save_upload function of upload module in Drupal 8.	
Source	https://www.aon.com/cyber-solutions/aon_cyber_labs/file-upload-vulnerability-in-drupal8/
Infected Technology	Drupal 8
Recommendation	Update the security patch available

2. LifeLabs Suffers Data Breach

Description	
LifeLabs the Health care Laboratory testing company in Canada suffers the massive data breach as an unknown attacker unauthorized accessed its computer system. The data breach exposed the personal and medical information of nearly 15 million canadians customers. An unknown attacker stole the data in a ransomware style malware with data ex-filtration abilities. The stole customers information not only includes names, address and DoB but also email address, login information, health card numbers, password for their lifelabs account and lab test results.	
Source	https://thehackernews.com/2019/12/lifelabs-data-breach.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2137.qx0ao0e5ow.1c12
Infected Industry	Health care Laboratory
Recommendation	Advised To change their passwords on the company's website as well as on any other site they have use same password

3. **This Bug Could Have Let Anyone Crash WhatsApp Of All Group Members**

Description	
A new vulnerability was identified in world's most popular messaging application WhatsApp, which could let an attacker to trigger a fully-destructive WhatsApp crash-loop, just by sending a maliciously crafted message to a targeted group. The group members can't even delete the malicious message without opening the group window and re-triggering the crash-loop , they have to lose the entire group chat history. This explioit works smoothly against all vulnerable Android users and iOS users.	
Source	https://thehackernews.com/2019/12/whatsapp-group-crash.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2137.qx0ao0e5ow.1c1k
Infected Technology	WhatsApp
Recommendation	Update the patch when available

4. **PayPal Phishing Attack Promises To Secure Accounts, Steals Everything**

Description	
Paypal customers are facing suspicious logins from unknown devices and attempting to squeeze them dry of all their credentials and financial info as the phishers attempting to trick users into handing over their access credentials to the payment service. The victims were tricked to click on the link embedded within the phishing message, which costs them to handover their credentials to the phishers.	
Source	https://www.bleepingcomputer.com/news/security/paypal-phishing-attack-promises-to-secure-accounts-steals-everything/
Infected Technology	Paypal
Recommendation	User awareness training on phishing mail

5. **Remote Code Execution via Insecure Deserialization in Telerik UI**

Description	
Telerik UI - a widely used suite of UI components for web applications- suffers an arbitrary remote code execution on software's underlying host as it insecurely deserialize JSON object. This vulnerability affects the internet-facing instances of Telerik UI as the modification on object rauPostData allows an attacker to control object's behaviour while its being deserialized which let an attacker perform remote code execution via insecure deserialization.	
Source	https://know.bishopfox.com/research/cve-2019-18935-remote-code-execution-in-telerik-ui
Infected Technology	Telerik
Recommendation	Update the patch when available

For any queries/recommendations:

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