InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. **Windows O-Day Exploited in Ransomware Attacks Apple iTunes and iCloud**
2. **Impreva Blames data Breach on Stole AWS API Key**
3. **DLL Loading Issues Opens PCs to Code Execution Attacks**
4. **SIM card in 29 countries Vulnerable To Remote Simjacker Attacks**
5. **7-year-old Critical RCE Flaw Found in Popular iterms2 macOS Terminal App**

13/10/2019

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. **Windows O-Day Exploited in Ransomware Attacks Apple iTunes and iCloud**

Description	
The cybercriminal group has been found exploiting a zero-day vulnerability in Windows through Unquoted service path in Apple's Bonjour service affecting a little-known component that comes bundled with Apple's iTunes and iCloud software for windows. This unquoted service path vulnerability enables a software security flaw that results exploitation by planting a malicious executable file to the parent path, tricking legitimate and trusted applications into executing malicious programs to maintain persistence and evade detection.	
Source	https://thehackernews.com/2019/10/apple-bonjour-ransomware.html
Infected Technology	Windows
Recommendation	Immediately update the available patched

2. **Impreva Blames data Breach on Stole AWS API Key**

Description	
Imperva, a cyber security company experienced a security breach as a hacker stole its Amazon Web Services (AWS) API key from an internal system that was left accessible from the internet. The hacker used the AWS API key to access Imperva's cloud infrastructure, where found company's AWS Relational Database Service(RDS) used for testing.	
Source	https://www.zdnet.com/article/imperva-blames-data-breach-on-stolen-aws-api-key/
Infected Technology	Imperva's cloud infrastructure

3. DLL Loading Issues Opens PCs to Code Execution Attacks

Description	
Security researchers found a vulnerability in an open-source software called Open Hardware Monitor. This software monitors temperature sensors, fan speeds, voltages and clock speeds of computers. It is also used by HP Touchpoint Analytics and utilized by millions of computers worldwide. If exploited, attackers with administrative privileges can execute arbitrary code on victims' systems. The main attack vector is DLL hijacking. Once the vulnerable software is loaded, it launches a third party library. The program doesn't validate whether the DLL being loaded is signed or not. Hence capable of loading any arbitrary unsigned DLL.	
Source	https://threatpost.com/hp-touchpoint-analytics-opens-pcs-to-code-execution-attack/149069/
Infected Technology	HP
Recommendation	Installed third party open source software with verification
CVE ID	CVE-2019-6333

4. SIM card in 29 countries Vulnerable To Remote Simjacker Attacks

Description	
Millions of active SIM cards in at least 29 countries (issued by a total of 61 operators) are vulnerable to remote hacking. Nearly 25,000 malicious messages were sent to 1500 unique devices in a period of 31 days only.	
Source	https://thehackernews.com/2019/10/simjacker-vulnerability-exploit.html
Infected Technology	Mobile Phones
Recommendation	filtering can be implemented to intercept and block the illegitimate binary SMS messages

5. **7-year-old Critical RCE Flaw Found in Popular iterms2 macOS Terminal App**

Description	
A 7-year-old critical remote code execution vulnerability has been discovered in iTerm2 macOS terminal emulator app—one of the most popular open source replacements for Mac's built-in terminal app.the flaw can also be triggered using command-line utilities by tricking them into printing attacker-controlled content, eventually allowing attackers to execute arbitrary commands on the user's Mac computer.	
Source	https://thehackernews.com/2019/10/iterm2-macos-terminal-rce.html ?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2089.qx0ao0e5ow.1auw
Infected Technology	Mac OS
Recommendation	Patch immediately when available