September 21, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- Zerologon: Windows vulnerability enables domain takeover
- Firefox lets attacker in network attacker hijack your Android device
- Spammer using hexadecimal IP addresses to evade detection
- Safari Bug revealed after Apple delay patch
- XSS bug discovered in Ruby Gem
- Majority of Top cybersecurity organization have leaked data on dark web
- Bluetooth Reconnection Issues

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. Zerologon: Windows vulnerability enables domain takeover

Description	
Microsoft has recently patched a privilege elevation vulnerability. The vulnerability dubbed Zerologon can be exploited using Microsoft's Netlogon Remote Protocol. The attack can be exploited by local unauthenticated attacker using MS-NRPC allowing him/her administrator access. Microsoft has released a patch modifying how Netlogon handles the usage of Netlogon secure channel. Second phase of the patch will only be available in Q1 of 2021.	
Source	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472
Infected Technology	Windows Server
CVE	CVE-2020-1472
Recommendation	Apply the security update released

2. Firefox lets attacker in network attacker hijack your Android device

Description	
Chris Moberly, security researcher at GitLab has identified a vulnerability in Firefox that allows attacker in your network to hijack your browser. The vulnerability resides in Firefox Simple Service Discover Protocol (SSDP) which allows users in same network to share and receive content. The SSDP components discovers device and accesses an XML file which can be used to hind malicious code. Moberly demonstrated the exploitation with use of *intent* command that execute commands. Mozilla has fixed the vulnerability in Firefox 79.	
Source	https://gitlab.com/gitlab-com/gl-security/security-operations/gl-redteam/red-team-tech-notes/-/tree/master/firefox-android-2020
Infected Technology	Firefox for Android
Recommendation	Update to the latest version

3. Spammer using hexadecimal IP addresses to evade detection

Description	
Spammer are now using hexadecimal instead of domain address to bypass email filters and security system. According to research report by Trustwave, spam groups are now using hexadecimal IP address. The hexadecimal IPs are interpreted by browser to convert to destination IP while security systems in placed has failed to detect them allowing more spam mail to be dropped to inbox.	
Source	https://www.zdnet.com/article/spammers-use-hexadecimal-ip-addresses-to-evade-detection/
Infected Technology	Windows
Recommendation	Do not open attachments from unknown sources Tune spam filter to identify hexadecimal IP address

4. Safari Bug revealed after Apple delay patch

Description	
Researcher from Cisco Talos has identified a remote code execution vulnerability Apple's Safari web browser. The vulnerability resides in the browser's Webkit feature. Attacker could trigger a use-after-free condition in WebCore, DOM-rendering system for Webkit allowing execution of code. Apple has released the patch for the vulnerability on Wednesday.	
Source	https://talosintelligence.com/vulnerability_reports/TALOS-2020-1124
Infected Technology	Safari Web Browser
Recommendation	Update the browser with latest security patched.

5. XSS bug discovered in Ruby Gem

Description	
A potential cross-site scripting (XSS) bug has been discovered in Action View, a popular Ruby Gem responsible to handle web requests in Rails web application framework. The vulnerability is in Action View's translation helper. The Action View passes an HTML-unsafe string and is marked as HTML-safe and not escaped. This allows attacker to disguise malicious code as legitimate. The issue has been patched in Rails version 6.0.3.3 and 5.2.4.4 , as well as the project's master, 6-0-stable and 5-2-stable branches on GitHub while workarounds for existing versions are also available.	
Source	https://portswigger.net/daily-swig/action-view-xss-bug-discovered-in-popular-ruby-gem
Infected Technology	Rails Web Application Framework
Recommendation	Apply the patch or workaround

6. Majority of Top cybersecurity organization have leaked data on dark web

Description	
A report has detailed how the majority of the world's top cybersecurity companies have had their data exposed on the dark web. The survey, from application Security firm ImmuniWeb, took a sample of nearly 400 of the largest cybersecurity companies from 26 countries across the globe, with the majority based in the US and Europe. The company, which uses AI to detect security issues, then used its own systems to discover and classify dark web data leaks related to those security organizations. It found that 97% had leaked data available on the dark web. In addition, 25% of incidents were classified as a 'high' or 'critical' risk level – meaning personally identifiable information had been exposed. Further data identified that 29% of leaked passwords belonging to the security companies were weak, and that employees from 40% of the organizations had reused credentials across different online services. ImmuniWeb also wrote that 91 of the companies studied had a security vulnerability present on their websites – 26% of which are yet to be fixed.	
Source	https://www.immuniweb.com/blog/state-cybersecurity-dark-web-exposure.html
Infected Areas	Retail websites, gaming platform, Dating site

7. Bluetooth Reconnection Issues

Description	
Billions of smartphones, tablets, laptops, and IoT devices are using Bluetooth software stacks that are vulnerable to a new security flaw disclosed over the summer. The Vulnerability BLESA (Bluetooth Low Energy Spoofing Attack), the impacts devices running the Bluetooth Low Energy (BLE) protocol. BLE is a slimmer version of the original Bluetooth (Classic) standard but designed to conserve battery power while keeping Bluetooth connections alive as long as possible. Due to its battery-saving features, BLE has been massively adopted over the past decade, becoming a near-ubiquitous technology across almost all battery-powered devices. We exploit the design weaknesses identified through the formal verification to craft the BLE Spoofing Attack (BLESA). In this attack, an adversary provides spoofed data to a client device pretending to be a previously paired server device.	
Source	https://www.usenix.org/system/files/woot20-paper-wu-updated.pdf
Infected Technology	Bluetooth
Recommendation	• Improve BLE Stack Implementation • Update the BLE specification

For any queries/recommendations:

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