May 18, 2020

INFOSEC WEEKELY

#MADE4SECURITY

- 3rd-Party RDP Clients Vulnerable after Improper Microsoft Patch
- CISCO & Palo Alto Network appliances impacted by Kerberos authentication bypass
- New Microsoft 365 sign-in pages spoofed for phishing
- Critical WordPress plugin bug allows for automated takeovers
- U.S. Defense warns of 3 new malwares used by North Korean Hacker
- Russian Hacker Group Using HTTP status code to control Malware Implant
- Android Apps exposing user data via Misconfigured Firebase

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, Trip Advisor, 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. WordPress Malware finds WooCommerce sites for Magecart attacks

Description	
Security researchers from Sucuri have a new WordPress malware used by threat actors to scan for and identify WooCommerce online shops with a lot of customers to be targeted in future Magecart attacks. The threat actors are taking advantage of security vulnerabilities found in other WordPress plugins to drop the malware. When this is exploited, attackers can access e-store's internal structure, discover if the site is using the WooCommerce platform and exfiltrate info that can let attackers gain control over the web server. The malware is installed in the form of malicious PHP script as a part of post exploitation.	
Source	https://www.bleepingcomputer.com/news/security/wordpress-malware-finds-woocommerce-sites-for-magecart-attacks/
Infected Technology	Vulnerable WooCommerce
Recommendation	Periodically update your site build on CMS and verify plugins before installing them.

2. CISCO & Palo Alto Network appliances impacted by Kerberos authentication bypass

Description	
Cisco and Palo Alto Networks seems to have a high-risk authentication bypass vulnerability that is caused by the incorrect implementation of Kerberos protocol. Threat actors can gain the administrative control by executing a Man-in-the-Middle (MitM) attack. Palo Alto Networks states, by spoofing vulnerability exists in the authentication daemon and User-ID components of Palo Alto Networks PAN-OS by failing to verify the integrity of the Kerberos key distribution center (KDC). A similar vulnerability also exists in the CISCO's ASA Software where it was exploitable if they had Kerberos authentication configured for VPN or local device access.	
Source	https://www.csoonline.com/article/3543838/cisco-and-palo-alto-networks-appliances-impacted-by-kerberos-authentication-bypass.html?&web_view=true
Infected Technology	CISCO & Palo Alto Devices
CVE	CVE-2020-2002, CVE-2020-3125
Recommendation	Validate if the Kerberos requires password or a keytab. Use third party libraries properly.

3. New Microsoft 365 sign-in pages spoofed for phishing

Description	
Attackers are running phishing campaigns for the newly updated designs for Azure AD and Microsoft 365 sign-in-pages. One of these recent phishing campaigns is delivering emails with the 'Business Document Received' subject line and PDF attachments that attempt to pass as OneDrive documents that require the potential victims to sign in for viewing. Another highly convincing series of phishing attacks were observed while using cloned imagery from automated Microsoft Teams notifications to harvest Office 365 credentials from tens of thousands of potential victims.	
Source	https://www.bleepingcomputer.com/news/security/new-microsoft-365-sign-in-pages-already-spoofed-for-phishing/?&web_view=true
Infected Technology	Microsoft 365
Recommendation	Always validate links before signing in

4. Critical WordPress plugin bug allows for automated takeovers

Description	
Attackers can exploit a critical vulnerability in the WP Product Review Lite plugin installed on over 40,000 WordPress sites to inject malicious code and potentially take over vulnerable websites. Attackers are also able to bypass user input sanitization function to launch Stored XSS where on successful exploitation allows them to inject malicious scripts in all the products stored in the site's database. Thousands of sites still are affected by this vulnerability.	
Source	https://www.bleepingcomputer.com/news/security/critical-wordpress-plugin-bug-allows-for-automated-takeovers/?&web_view=true
Infected Technology	WordPress plugin
Recommendation	Upgrade to the latest release of their plugin

5. U.S. Defense warns of 3 new malwares used by North Korean Hacker

Description	
Cybersecurity and Infrastructure Security Agency (CISA) with FBI and Department of Defense released a joint advisory regarding 3 new malwares used by state-sponsored North Korean hackers. The malware dubbed COPPERHEDGE, TAINTEDSCRIBE, and PEBBLEDASH are capable of remote reconnaissance and exfiltration of sensitive information. Theses malwares are addition to existing list of over 20 malware samples identified as part of series of malicious cyber activities named *Hidden Cobra* by the *Lazarus Group*. These malware**s** are used as Remote Access Tool (RAT) and backdoor imitating Microsoft's Narrator utility.	
Source	https://thehackernews.com/2020/05/fbi-north-korean-malware.html
Infected Medium	
Recommendation	Use proper layered defense to detect anomalies in your systems and network.

6. 3rd-Party RDP Clients Vulnerable after Improper Microsoft Patch

Description	
There was one vulnerability that surfaced with the name 'Reverse RDP Attack, wherein a client system vulnerable to a path traversal vulnerability could get compromised when remotely accessing a server over Microsoft's Remote Desktop Protocol. Though Microsoft had patched the vulnerability (CVE-2019-0887) as part of its July 2019 Patch Tuesday update, it turns out researchers were able to bypass the patch just by replacing the backward slashes in paths with forward slashes. Microsoft acknowledged the improper fix and re-patched the flaw in its February 2020 Patch Tuesday update earlier this year, now tracked as CVE-2020-0655.	
Source	https://research.checkpoint.com/2020/reverse-rdp-the-path-not-taken/
Infected Technology	Microsoft RDP
CVE	CVE-2020-0655, CVE-2019-0887
Recommendation	Update to the latest patch provided by Microsoft

7. Thunderbolt vulnerability allows file access in devices before 2019

Description	
Björn Ruytenberg, a security researcher from Eindhoven University of Technology, has discovered a flaw in thunderbolt enabled devices manufactured before 2019 which allows attack called "Thunderspy". The vulnerability allows attacker to retrieve the computer data in minutes when physical access is available. The issue is found in all Windows and Linux machines with thunderbolt ports and partially affects Mac devices as well. According to the researcher, patching the vulnerability requires hardware redesign and cannot be done via software update which makes it persistent.	
Source	https://threatpost.com/millions-thunderbolt-devices-thunderspy-attack/155620/
Infected Technology	Thunderbolt ports
Recommendation	Disable Thunderbolt ports in BIOS if not used. Do not leave devices unattended.

8. Russian Hacker Group Using HTTP status code to control Malware Implant

Description	
Security researchers have identified a new version of the COMpfun malware that controls infected hosts using a mechanism that relies on HTTP status codes. Responsible for the attacks is a group known as Turla, a state-sponsored Russian threat actor that has historically engaged in cyber-espionage operations. Turla has a long history of using non-standard and innovative methods to build malware and carry out stealthy attacks.	
Source	https://thehackernews.com/2020/05/malware-http-codes.html
Infected Sectors	Governments, embassies, military, education, research, and pharmaceutical companies.

9. Android Apps exposing user data via Misconfigured Firebase Databases

Description	
An investigation by Security Discover with partnership with Comparitech identified over 4,000 Android apps were accidently leaking sensitive information of users including email addresses, username, passwords, phone numbers, chat messages and location data. These applications used misconfigured Firebase databases which disclosed the information. Since Firebase is cross platform tool, the misconfiguration is likely to impact iOS and web apps as well. Besides leaking information, thousands of application**s** had write permission allowing attacker to inject malicious code to spread malware. Google has been notified of the issue and has been reaching out to developers to fix patch the issue	
Source	https://thehackernews.com/2020/05/android-firebase-database-security.html
Infected Technology	Firebase Database
Recommendation	Follow best practices while building application

For any queries/recommendations:
Contact us: **whois@cryptogennepal.com**