December 28, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- Critical Bug in Del Wyse
- QNAP fixes high severity QTS, QES, and QuTS hero vulnerabilities
- Trust-Based Federated Login Abused for Local-to-Cloud Attacks
- pay2Key Ransomwares' Mayhem Continues
- Microsoft warns Azure Cloud Customers regarding CrowdStrike of Hackers
- Attackers Abusing Citrix NetScaler Devices to Launch Amplified DDoS Attacks
- Google Discloses Poorly patched Windows zero-day Bug

CryptoGen Nepal

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. Critical Bug in Del Wyse

Description

Dell has patched two critical security vulnerabilities in its Dell Wyse Thin Client Devices, which are small form-factor computers optimized for connecting to a remote desktop. The bugs allow arbitrary code execution and the ability to access files and credentials. As for how many devices are potentially impacted, it's unclear — but Dell has said in the past that there are "millions" of Dell Wyse Thin Clients deployed within organizations. One of the main reasons this vulnerability is critical is that its attack complexity is very easy. All it takes is uploading an altered text configuration file to a configuration server via FTP and No authentication to the thin client is required; the only possible authentication is with the FTP server (for the uploading the configuration), but by default it is installed with no credentials.

Source	https://threatpost.com/critical-bugs-dell-wyse-thin-clients/162452/
Infected Technology	Dell Laptops
CVE_ID	CVE-2020-29491, CVE-2020-29492
Recommendation	Apply the security patches provided by Dell.

2. QNAP fixes high severity QTS, QES, and QuTS hero vulnerabilities

Description

QNAP has released security updates to fix multiple high severity security vulnerabilities impacting network-attached storage (NAS) devices running the QES, QTS, and QuTS hero operating systems. In total, the NAS maker has patched six vulnerabilities affecting earlier version of its FreeBSD, Linux, and 128-bit ZFS based OSs. The issues in QNAP about command injection, cross site scripting (XSS), and hard-coded password were reported by TIM Security Red Team Research, Lodestone Security, and the CFF of Topsec Alpha Team.

Source	CVE-2020-2503, CVE-2020-2504, CVE-2020-2505 CVE-2016-6903, CVE-2020-2499, CVE-2020-25847
Infected Technology	QNAP's NAS devices running the QES, QTS, and QuTS hero
Recommendation	Apply security patches provided by QNAP
CVE	CVE-2020-2503, CVE-2020-2504, CVE-2020-2505, CVE-2016-6903, CVE-2020-2499, CVE-2020-25847

3. Trust-Based Federated Login Abused for Local-to-Cloud Attacks

Description	
In the light of SolarWinds supply chain attack, the National Security Agency described two different techniques used by cyber criminals to escalate access from hacked local networks to cloud-based infrastructure. According to NSA, these techniques are not new and have been in use since at least 2017. These two techniques are not based on the exploitation of any vulnerabilities in the federated authentication products, the SAML protocol, or the associated identity services but on the trust of the on-premises components that perform authentication, assign privileges, and sign SAML tokens. The attacks reportedly abused the legitimate functions after compromising a local network or admin account.	
Source	https://media.defense.gov/2020/Dec/17/2002554125/-1/-1/0/AUTHENTICATION_MECHANISMS_CSA_U_OO_198854_20.PDF
Infected Technology	SolarWinds
Recommendation	Apply the security patch provided by SolarWinds.

4. pay2Key Ransomwares' Mayhem Continues

Description	
The recently discovered Pay2Key ransomware is slowly emerging as a dangerous threat in the ransomware landscape. The ransomware, which made its first appearance in October, is actively targeting organizations leveraging the double extortion technique. The attackers used RDP connections to gain an initial foothold and to propagate across the entire network. After completing the infection phase, the attackers dropped a customized ransom note, with a relatively low demand of 7-9 bitcoins. The ransomware is only the latest wave in a series of Iranian based targeted ransomware attacks deployed against Israeli organizations and this appears to be a growing trend.	
Source	https://research.checkpoint.com/2020/ransomware-alert-pay2key/
Infected Technology	Systems using RDP
Recommendation	• Consider closing port 3389 where not necessary. • Update endpoint security solutions daily.

5. Microsoft warns Azure Cloud Customers regarding CrowdStrike of Hackers

Description	
Microsoft's Threat Intelligence Center identified a third-party reseller's Microsoft Azure account executing 'abnormal calls' to Microsoft cloud APIs on December 15. The affected reseller's Azure account handles Microsoft office licensing for its Azure customers that includes CrowdStrike.	
Source	https://www.crowdstrike.com/blog/crowdstrike-launches-free-tool-to-identify-and-help-mitigate-risks-in-azure-active-directory/
Infected Technology	Microsoft Azure Cloud
Recommendation	Use of utilities: CrowdStrike Reporting Tool for Azure (CRT) to review excessive permission in Azure Active Directory or Office 365 and Sparrow to detect compromised accounts and application

6. Attackers Abusing Citrix NetScaler Devices to Launch Amplified DDoS Attacks

Description	
Attackers are abusing a security issue in NetScaler application delivery controller (ADC) devices to launch amplified distributed denial-of-service (DDoS) attacks against several targets. An attacker or bots can overwhelm the Citrix ADC [Datagram Transport Layer Security] network throughput, potentially leading to outbound bandwidth exhaustion. The issue came to light after multiple reports of a DDoS amplify attack over UDP/443 against Citrix (NetScaler) Gateway devices at lease since December 19.	
Source	https://www.zdnet.com/article/citrix-devices-are-being-abused-as-ddos-attack-vectors/
Infected Technology	Citrix's NetScaler Application Delivery Controller (ADC)
Recommendation	Continuously monitor the outbound traffic volume for any significant anomaly or spikes.

7. Kaspersky reports dangerous Chrome extensions

Description	
Kaspersky in collaboration with Yandex reported more than twenty browser extensions working on Chrome for the malicious user. The extensions had been installed in more than 8 million browsers and would access remote server, download malicious code and execute processes tagged dangerous by the security solutions. The attackers had used these extensions to generate traffic to videos by secretly playing in an invisible video player that was only activated when the user was browsing. The plugins would also intercept access to social networking for inflating counts of undisclosed subjects.	
Source	https://www.kaspersky.com/blog/chrome-plugins-alert/38242/
Infected Technology	Google Chrome
Recommendation	Install antivirus. Disable plugins detected malicious by security application.

8. Google Discloses poorly patched Windows zero-day Bug

Description	
Google Project Zero team has disclosed the detailed information of an improperly patched zero-day vulnerability in Windows Print Spooler API that could leads to execute arbitrary code by attacker. An attacker must first obtain the ability to execute low-privileged code on the target to exploit this vulnerability. The flaw exists within the user-mode printer driver host process splwow64.exe. The issue results from the lack of proper validation of a user-supplies value prior to dereferencing it as a pointer.	
Source	https://www.zerodayinitiative.com/advisories/ZDI-20-663/
Infected Technology	Microsoft Windows
Recommendation	Workaround: Apply necessary policy to restrict interaction with vulnerable service
CVE	CVE-2020-0986, CVE-2020-17008

9. New AridViper Malware Targets Outlook Users

Description	
Palo Alto's Unit42 research team has recently found hacking group AridViper (aka APT-C-23) dropping a new malware to target victims in the Middle Eastern region. This was discovered while investigating AridViper's Micropsia malware. The newly developed Python-based malware—called PyMicropsia—has several information-stealing and control capabilities such as keylogging, downloading and executing payloads, stealing browser credentials, clearing browsing history and profiles, rebooting machines, collecting Outlook processes, and many more. The trojan also contains both built-in Python libraries and specific packages including PyAudio and mss for multiple purposes including information-stealing, interacting with Windows processes, networking, file system, Windows registry, and so on.	
Source	https://unit42.paloaltonetworks.com/pymicropsia/
Infected Technology	Microsoft Outlook
Recommendation	Install endpoint security solutions to detect Malwares. Monitor network traffic continuously.

10.Man-in-the-Middle vulnerability in Kubernetes

Description	
Kubernetes Product Security Committee had disclosed a vulnerability with medium severity. The vulnerability was affecting all Kubernetes versions allowing a Kubernetes Service design flow to intercept cluster traffic on any IP address. A user could exploit this vulnerability by carrying out a man-in-the-middle attack against pods and nodes. The user could tamper the victim data, harvest credentials from the network traffic, block communication with a specific IP and masquerade as internal and external endpoints.	
Source	https://unit42.paloaltonetworks.com/cve-2020-8554/
Infected Technology	Kubernetes
Recommendation	Update the system as soon as the patch is released, prevent the use of external IPs.
CVE	CVE-2020-8554

For any queries/recommendations:

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