August 16, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Windows 365 exposes Azure credentials in plain text
- Yet another vulnerability in Windows Print Spooler
- 0-day RCE in Cisco Adaptive Security Device Manager
- Nine Critical and High-Severity Vulnerabilities Patched in SAP Products
- Authenticated RCE and privilege Escalation Vulnerability on cPanel & WHM

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.

Windows 365 exposes Azure credentials in plain text

Description	
Benjamin Delpy, security researcher and creator of Mimikatz, have identified a way to dump Microsoft Azure credentials from Windows 365 Cloud PC. Benjamin used Mimikatz and previously identified flaw in Windows to dump the plain text credential for user logged in via Terminal session. While the credential is encrypted the memory, the tools tricks terminal service to request decryption to the kernel. While the execution of the tool requires Administrative execution in the victim PC, a pre-infected device can be used to gain access to Azure credentials.	
Source	https://www.bleepingcomputer.com/news/microsoft/windows-365-exposes-microsoft-azure-credentials-in-plaintext/?&web_view=true
Infected Technology	Windows 365

Yet another vulnerability in Windows Print Spooler

Description	
Microsoft has released an advisory for a new flaw in its print spooler service after releasing an update to patch the existing vulnerability last week. The newly disclosed vulnerability exists due to improper privileged file operation. Exploitation of the vulnerability could allow attacker to execute arbitrary code execution with system privilege allowing installation of new programs, modify and add user accounts. Microsoft has requested to disable print spooler service as workaround to prevent exploitation of the vulnerability.	
Source	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36958
Infected Technology	Microsoft
Recommendation	Update the latest available patch
CVE-ID	CVE-2021-34473, CVE-2021-34523, CVE-2021-31207

o-day RCE in Cisco Adaptive Security Device Manager

Description	
Cisco has released a security advisory revealing the Remote code execution bug in Cisco Adaptive Security Device Manager Launcher. The vulnerability exists due to a lack of signature verification between ADSM and Launcher for specific code. An attacker can exploit the vulnerability by launching man-in-the-middle attack between Launcher and ADSM allowing injection of arbitrary code. The exploit allows execution of arbitrary code in victim's OS with privilege provided to ADSM Launcher. The vulnerability has not been patched and no workaround has been provided by OEM until now.	
Source	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asdm-rce-gqjShXW
Infected Technology	Cisco ADSM 7.16(1.150) and earlier
Recommendation	Update the patch once released by OEM
CVE-ID	CVE-2021-1585

Nine Critical and High-Severity Vulnerabilities Patched in SAP Products

Description	
Onapsis stated in a blog that with the nine critical patches in total, The critical vulnerability that was patched by SAP includes SSRF affecting Netweaver development infrastructure, an unrestricted file upload problem affectiong SAP buisness One and SQL injection in DMIS Plug-in. The high-severity vulnerability that was patched by SAP includes two XSS flaws and an SSRF issue in the NetWeaver Enterprise Portal.	
Source	https://onapsis.com/blog/sap-security-patch-day-august-2021
Infected Technology	SAP Products
Recommendation	Update the latest available patch released by OEM
CVE-ID	CVE-2021-33698, CVE-2021-33690, CVE-2021-33701

Authenticated RCE and privilege Escalation Vulnerability on cPanel & WHM

Description	
cPanel & WHM is a suite of Linux tools that enable the automation of web hosting tasks via a graphical user interface (GUI). cPanel is used when hosting more than 168,000 websites, according to Datanyze. During a black box pen test, RCE was also demonstrated via a "more intricate" CSRF bypass chained to a cross-site WebSocket hijacking attack. The web hosting firm has not fixed these flaws – it only patched a separate, XXE vulnerability – because attackers must be authenticated with a reseller account with permission to edit locales, which is not a default configuration.	
Source	https://www.fortbridge.co.uk/research/multiple-vulnerabilities-in-cpanel-whm/
Infected Technology	cPanel & WHM
Recommendation	Update the latest available patch.

Trend Micro issues warning for zero-day attacks

Description	
Cyber-security firm Trend Micro said hackers tried to exploit two zero-day vulnerabilities in its Apex One EDR platform to go after its customers in attacks that took place earlier this year. While details about the attacks are currently being kept under wraps, patches for both issues were made available. Trend Micro said the two zero-days appear to have been used together in an exploit chain where the hackers uploaded malicious code on Apex One platforms and then elevated their access to gain control over the host system.	
Source	https://securityaffairs.co/wordpress/121082/security/trend-micro-zero-day-attacks.html?web_view=true
Infected Technology	Trend Micro Apex one
Recommendation	Update the patch released
CVE-ID	*CVE-2021-32464, CVE-2021-32465, CVE-2021-26741*, and *CVE-2021-36742*.

Updated AdLoad Malware Capable of Bypassing Apple's Defenses

Description	
XProtect, Apple's built-in YARA signature-based malware detection antivirus tech solution can be bypassed by a new variant of AdLoad malware. Out of over 220 samples, researchers have observed that 150 were not detected by XProtect. After the adware infects a Mac, it hijacks the search engine results by installing a Man-in-the-Middle (MITM) web proxy. Ads are then administered to web pages for financial gain. Also, LaunchDaemons and LaunchAgents are installed on compromised Macs. User cron jobs are executed every two and a half hours in some instances.	
Source	https://cyware.com/news/updated-adload-malware-capable-of-bypassing-apples-defenses-ad1eaa37
Infected Technology	macOS platform

Apple fixes AWDL bug that could be used to escape air-gapped networks

Description	
A vulnerability in Apple's wireless Direct Link (AWDL) technology that could allow perpetrators to use ICMPv6 and IPv6 packets to take data from an infected system, bounce the packets on a nearby AWDL-capable Apple device, and send the stolen files to another device with an IPv6 address had been patched in April and has been publicly disclosed in August. Apple's AWDL protocol allows apple devices to talk to each other through Bluetooth or WIFI	
Source	https://therecord.media/apple-fixed-awdl-bug-that-could-be-used-to-escape-air-gapped-networks/?web_view=true
Infected Technology	Apple Devices
Recommendation	Update the patch released. The patches have been issued in iOS 14.5, iPadOS 14.5, watchOS 7.4, and Big Sur 11.3.

For any queries/recommendations:

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

OUR SERVICES

Our services as information security company includes:


INFORMATION SECURITY AUDIT


VULNERABILITY ASSESSMENT


PENETRATION TESTING


MANAGED/CO.MANAGED SOC


INCIDENT RESPONSE


THREAT ANALYSIS


SERVER HARDENING


CYBER SECURITY CONSULTANT


INFORMATION SECURITY TRAINING

CryptoGen Nepal

https://www.facebook.com/CryptoGenNepal/
https://twitter.com/CryptoGenNepal
https://www.instagram.com/CryptoGenNepal/