INVINSENSE™
Attacktical Cybersecurity Sense

Infopercept

INFOPERCEPT NEWSLETTER

ISSUE -12 July 2021

Contents

TO COMPETENTLY PERFORM RECTIFYING SECURITY SERVICE, TWO CRITICAL INCIDENT RESPONSE ELEMENTS ARE NECESSARY: INFORMATION AND ORGANIZATION.

Patches Notes

QNAP FIXES CRITICAL BUG IN NAS BACKUP, DISASTER RECOVERY APP

- NAS device of QNAP has a critical security vulnerability enabling attackers to compromise vulnerable NAS devices' security.
- The security issue is caused by buggy software that does not correctly restrict attackers from gaining access to system resources allowing them escalate privileges, execute commands remotely, or read sensitive info without authorization.

MICROSOFT ISSUES EMERGENCY PATCH FOR CRITICAL WINDOWS PRINTNIGHTMARE VULNERABILITY

- Microsoft issues critical out-of-band security update to address a critical zero-day vulnerability — known as "PrintNightmare" — that affects the Windows Print Spooler service and can permit remote threat actors to run arbitrary code and take over vulnerable systems.
- Tracked as CVE-2021-34527 (CVSS score: 8.8), the remote code execution flaw impacts all supported editions of Windows. Last week, the company warned it had detected active exploitation attempts targeting the vulnerability.

KASEYA PATCHES IMMINENT AFTER ZERO-DAY EXPLOITS, 1,500 IMPACTED

- The worldwide July 2 attacks on the Kaseya Virtual System/Server Administrator (VSA) platform by the REvil ransomware gang turn out to be the result of exploits for at least one zero-day security vulnerability, and the company is swinging into full mitigation mode, with patches for the on-premise version coming sometime this week, it said.
- That MSP connection allowed REvil access to those customers-of-customers, and there are around 1,500 downstream businesses now affected, Kaseya said in an updated rolling advisory.

CYBER ATTACKS

ANDROID-APPS STEALING FACEBOOK CREDENTIALS

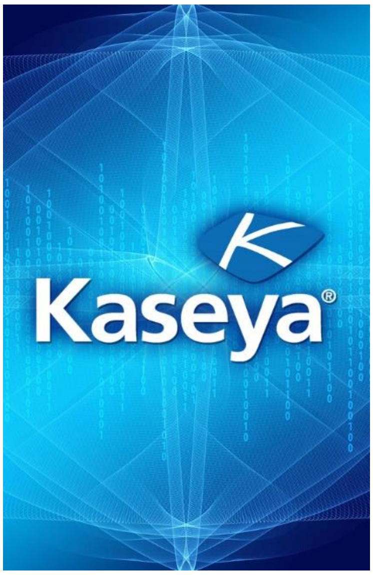
- Google interfere in removing nine Android apps downloaded more than 5.8 million times from the company's Play Store after the apps were caught furtively stealing users' Facebook login credentials.

- The offending apps masked their malicious intent by disguising as photo-editing, optimizer, fitness, and astrology programs, only to trick victims into logging into their Facebook accounts and hijack the entered credentials via a piece of JavaScript code received from an adversary-controlled server.

INDIAN TECH EXPOSES BYJU'S STUDENT DATA

- India-based technology startup Salesken.ai has secured an exposed server that was spilling private and sensitive data on one of its customers, Byju's, an education technology giant and India's most valuable startup.

- The server was left unprotected since at least June 14, according to historical data provided by Shodan, a search engine for exposed devices and databases. Because the server was without a password, anyone could access the data inside.



FAKE KASEYA ON GOING PHISHING CAMPAIGN

- Customers have been warned by Kaseya that a phishing campaign is attempting to access their networks by sending emails with malware attachments and embedded links posing as genuine VSA security upgrades.

- The attackers gain persistent remote access to the already compromised computers whenever the victim open the malicious attachment or download and run the fake Microsoft update...

69K LIMEVPN HACKED DATA SALE ON DARK WEB

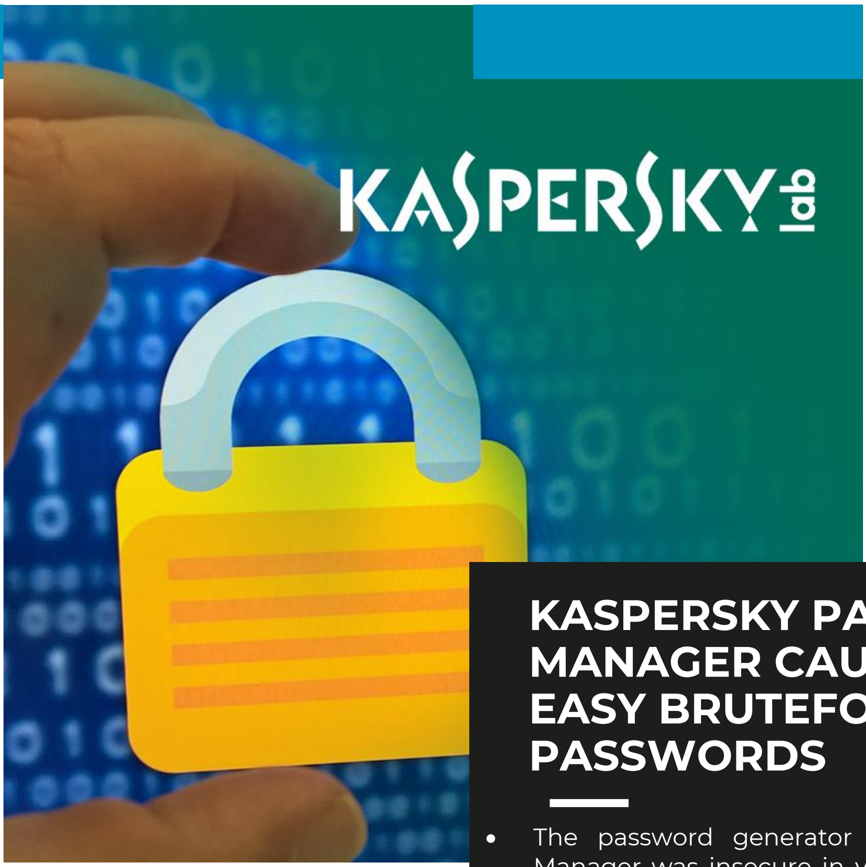
- The VPN provider known as LimeVPN has been hit with a hack affecting 69,400 user records, according to researchers.

- A hacker claims to have stolen the company's entire customer database before knocking its website offline). The stolen records consist of user names, passwords in plain text, IP addresses and billing information, according to PrivacySharks. Researchers added the attack also included public and private keys of LimeVPN users.

Malware and Vulnerabilities

WESTERN DIGITAL USERS FACE ANOTHER RCE

- The latest zero-day entails an attack chain that allows an unauthenticated intruder to execute code as root and install a permanent backdoor on the vendor's network-attached storage (NAS) devices.
- Latest bug, reported last week is a third, similarly serious zero-day vulnerability in a much broader range of newer Western Digital My Cloud NAS boxes.



KASPERSKY PASSWORD MANAGER CAUGHT OUT TO BE EASY BRUTEFORCED PASSWORDS

- The password generator feature in Kaspersky Password Manager was insecure in various ways because the security vendor failed to follow well understood cryptographic best practices, it has emerged.
- The multiple flaws – tracked as CVE-2020-27020 – were discovered in June 2019 but were only patched in October 2020. Users were told to update to Kaspersky Password Manager 9.0.2 Patch M and re-generate passwords. That in itself didn't completely fix the issue because the mobile version of the software was still vulnerable until that too was addressed and an advisory published in April 2021.

NETGEAR ROUTERS FIRMWARE VULNERABILITIES EXPOSES NETWORK SECURITY RISK

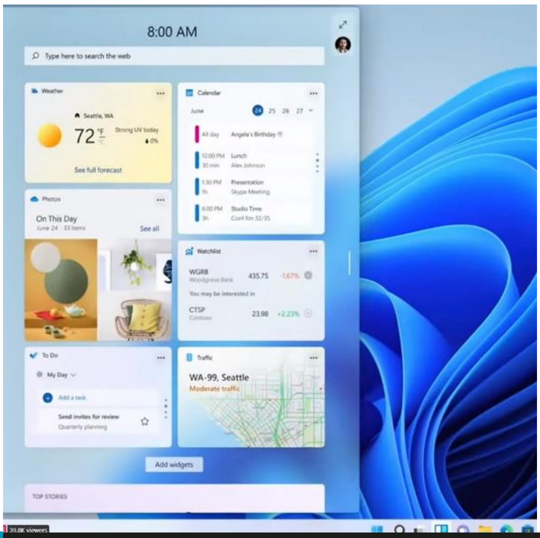
- Firmware vulnerabilities in a commercial-grade Netgear router opened the door to a range of exploits, including identity theft and full system compromise.
- The three flaws present an accessing router management pages using authentication bypass risk, the possibility of deriving saved router credentials via a cryptographic side-channel and a flaw that made it possible to retrieve secrets stored in the device thanks to use of default cryptographic key, respectively.

CYBER TECH

GOOGLE CHROME WILL GET AN HTTPS-ONLY MODE FOR SECURE BROWSING

- Google is working on adding an HTTPS-Only Mode to the Chrome web browser to protect users' web traffic from eavesdropping by upgrading all connections to HTTPS.

- Google has previously updated Chrome to default to HTTPS for all URLs typed in the address bar if the user specifies no protocol.



WINDOWS 11 WITH NEW FEATURES AND BUGS FIXES RELEASE NOTE

- Microsoft adds new features and fixed multiple bugs/issues in the latest Windows 11 Dev build based on feedback received from Windows Insiders in the Dev Channel. The company officially unveiled Windows 11 as the next version of Windows last month, saying that Windows Insiders would first get a taste preview builds.

- Among the most important new additions, the Start menu now comes with a search box to make it easier to find files, and the taskbar can now be configured to show across multiple displays.

SOPHOS INCREASES PROTECTION WITH ADDITION TO CAPSULE8 FOR LINUX SECURITY

- Sophos has bought Capsule8 in order to improve its own protection of Linux systems.

- Later this fiscal year, Sophos will integrate Capsule8 technology, which focuses on Linux cyber security, into its Adaptive Cybersecurity Ecosystem to provide Linux server and cloud container security.

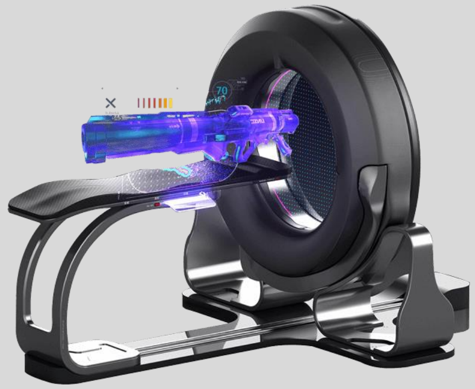
Infopercept

ABOUT INFOPERCEPT

Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Our specialized core team comprises experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, latest trends, and security innovations; ensuring that you always get the best security approach & solution for your specific business needs exactly the way you want it to be.

PROCESS ADVISORY SERVICES



What is a Security Maturity Assessment?

Infopercept's exceedingly experienced group will visit your site, directing a scope of meetings, workshops and tests with individuals over your business. From these exercises we will deliver start to finish investigation of your kin, procedures and devices, with our discoveries being displayed by means of:

A report - which incorporates abnormal state operational counsel and nitty gritty specialized direction to improve your security hazard pose. Our discoveries will be organized utilizing a traffic light framework so you know which territories require consideration first.

Infopercept
SECURE • OPTIMIZE • STRENGTHEN

+91 98988 57117
sos@infopercept.com
www.infopercept.com

INVINSENSE™
Attacktical Cybersecurity Sense