INVINSENSE™
Attacktical Cybersecurity Sense

Infopercept

INFOPERCEPT NEWSLETTER

ISSUE -27 September 2021

Contents

Patches Notes

APPLE FIXED TWO ZERO-DAY FLAWS LINKED TO PEGASUS

- Apple has issued a security bulletin to address two zero-day flaws that are now being exploited in active attacks. These weaknesses are tracked as CVE-2021-30860 and CVE-2021-30858 in iOS/macOS.
- The iPhones of nine activists from the Bahrain Center for Human Rights, Al Wefaq, and Waad were targeted in the attack.

NETGEAR FIXES DANGEROUS CODE EXECUTION BUG IN MULTIPLE ROUTERS

- Netgear has patched a high-severity remote code execution (RCE) vulnerability discovered in the Circle parental control programme, which runs with root privileges on almost a dozen current Netgear routers for Small Offices/Home Offices (SOHO).
- To achieve Remote Code Execution (RCE) as root on the targeted router, attackers must change network traffic or intercept traffic while on the same network to successfully exploit this vulnerability.

RESEARCHERS COMPILE LIST OF VULNERABILITIES ABUSED BY RANSOMWARE GANGS

- The ransomware gangs list has also been enlarged to include actively exploited holes that have been or are presently being abused by one or more ransomware groups in prior and ongoing assaults.
- Remote Code Execution (RCE) exploits targeting the recently fixed Windows MSHTML vulnerability have been used by an unidentified number of ransomware-as-a-service groups (CVE-2021-40444)

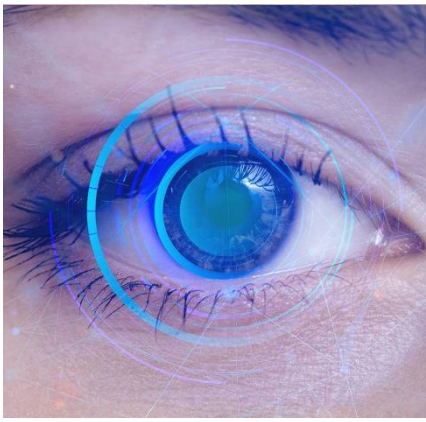
CYBER ATTACKS

PAYMENT API VULNERABILITIES EXPOSED "MILLIONS" OF USERS

- Researchers uncovered API security vulnerabilities impacting various apps, which might have exposed personal and payment information to millions of people.
- CloudSEK has discovered that a wide range of firms, both large and small, that serve millions of people have mobile apps with hardcoded API keys.

US OPTOMETRY PROVIDER SIMON EYE HIT BY DATA BREACH IMPACTING 144,000 PATIENTS

- According to a data breach alert on the Simon Eye website, unauthorised access to employee email accounts over a seven-day period between May 12-18, 2021, resulted in the possible compromise of sensitive personal data.
- Patients' identities, medical histories, treatment and diagnosis information, health insurance policy and/or subscriber information, and insurance application and/or claims information may have been exposed, according to a study of the compromised mailboxes' contents.



INDIA REPORTED 11.8% RISE IN CYBER-CRIME IN 2020

- In 2020, India registered 50,035 incidences of cyber-crime, an increase of 11.8 percent over the previous year, with 578 incidents of "false news on social media" being documented.
- According to the NCRB, there were 4,047 cases of online banking fraud, 1,093 OTP frauds, 1,194 credit/debit card frauds, and 2,160 cases of ATM fraud detected in 2020.

VOIP.MS PHONE SERVICES DISRUPTED BY DDOS EXTORTION ATTACK

- Threat actors are launching a DDoS attack against VoIP.ms and extorting the company to stop the attack, which is substantially impacting the company's operations.
- VoIP.ms transferred their website and DNS servers to Cloudflare to prevent the attacks, and while they reported some success, the company's site and VoIP infrastructure are still down owing to the ongoing denial-of-service attack.

Malware and Vulnerabilities

NEW MACOS ZERO-DAY BUG LETS ATTACKERS RUN COMMANDS REMOTELY

- Researchers discovered a new vulnerability in Apple's macOS Finder that allows attackers to execute instructions on Macs running any macOS version up to the most recent release, Big Sur.
- These files can be embedded in emails, and when the user clicks on them, the commands hidden within them are executed without prompting or notifying the user.

INSECURE HIKVISION SECURITY CAMERAS CAN BE TAKEN OVER REMOTELY

- Because the owner of the device is restricted to a limited protected shell (psh) that filters input to a predefined set of limited, largely informational commands, the critical defect allows the attacker to obtain even greater access than the owner.
- There is no requirement for the camera owner to do anything other than have access to the http(s) server port (usually 80/443). Any logging on the camera itself will not be able to detect the attack. By sending some communications with carefully written commands, a threat actor can use the vulnerability to initiate a command injection attack.

VMWARE WARNS OF CRITICAL FILE UPLOAD VULNERABILITY AFFECTING VCENTER SERVER

- Multiple severe security flaws in two VMware network management tools have been patched, allowing an attacker to gain complete control of an organization's network.
- A local privilege escalation vulnerability (CVE-2021-21991), a reverse proxy bypass vulnerability (CVE-2021-22006), and insufficient permission local privilege escalation vulnerabilities have all been discovered in vCenter Server (CVE-2021-22015).

CYBER TECH

OFFICE 2021 WILL BE AVAILABLE FOR NON-MICROSOFT 365 SUBSCRIBERS ON OCTOBER 5

- Dark Mode support, support for OpenDocument version 1.3, new Excel functions and formulas, enhanced slide show recording for PowerPoint, and many user-interface adjustments and additions are all included in the latest edition.
- For Office 2021, Microsoft intends to provide five years of "Mainstream Support" without any additional support. Support for Office 2021 will terminate in October 2026, barely a year after support for Office 2016 and Office 2019 for Windows would finish.

GOOGLE ANNOUNCES PARTNERSHIP TO REVIEW SECURITY OF OPEN-SOURCE SOFTWARE PROJECTS

- Google is supporting security examinations of eight projects through a partnership with the Open Source Technology Improvement Fund, after donating $100 million to improve open source security last month (OSTIF)
- In the OSSRA reports for 2021 and 2020, both the Jackson-databind component and Lodash were identified as highly vulnerable components in the majority of audited applications.

SRNL'S NEW FACILITY IN GEORGIA TO FOCUS ON CRITICAL INFRASTRUCTURE, ICS CYBERSECURITY; VAHID

- In Augusta, Georgia, the Savannah River National Laboratory (SRNL) has constructed a facility to conduct research on defending critical infrastructure and industrial control systems from cyber-attacks.
- The lab's cybersecurity team will have eight members at first, and it hopes to collaborate with groups like the Army Cyber Command, the Georgia Bureau of Investigation Cyber Crime Center, and Augusta University's School of Computer and Cyber Sciences.

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 & secur having good practical experienc 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.

INYINSENSE™ Attacktical Cybersecurity Sense

TECHNOLOGY ASSESSMENT SERVICES

All organizations are just a single data breach away from being the lead story on the news and social media, which can severely damage an organization's brand reputation. Regular security assessments helps in identifying your most significant vulnerabilities. You can thus cus on targeting opportunities for nprovement that offer the highest return on investment.

Infopercept's Technical Assessment Services provides key "inputs" of a security roadmap; where a thorough cyber security assessment evaluates your organizations's technology, policies, and awareness.

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