

Contents

01 Patches Notes

02 Cyber Attack

03 Malware and Vulnerabilities

04 Cyber-Tech

“

**TECHNOLOGY TRUST
IS A GOOD THING,
BUT CONTROL IS A
BETTER ONE.**



Patches Notes

WEIDMUELLER PATCHES DOZEN VULNERABILITIES IN INDUSTRIAL WLAN DEVICES

- The security holes impact wireless access point/bridge/client devices running firmware versions prior to 1.16.21 (build 21010513) or 1.11.13 (build 21010513).
- The vulnerabilities, tracked with the CVE identifiers CVE-2021-33528 through CVE-2021-33539, can be exploited for privilege escalation, decryption of traffic, arbitrary code/command execution, denial-of-service (DoS) attacks, and authentication bypass.



NVIDIA PATCHES HIGH-SEVERITY GEFORCE SPOOF-ATTACK BUG

- A vulnerability in NVIDIA's GeForce Experience software opens the door to remote data access, manipulation and deletion.
- NVIDIA notified customers late last week of the bug and released a software patch for the flaw, which is present in its GeForce Experience (versions 3.21 and prior) Windows software. The bug is tracked as CVE-2021-1073, with a CVSS severity rating of 8.3 (high).



WINDOWS 10 KB5004760 EMERGENCY UPDATE FIXES PDF OPENING ISSUE

- Microsoft has released an optional out-of-band update for all supported Windows 10 versions to address an issue preventing customers from opening PDF documents using some applications.
- The KB5004760 emergency update is available for devices running client editions of Windows 10 versions 2004, 20H2, and 21H1, as well as Windows Server versions 2004 and 20H2.



SECOND LINKEDIN "BREACH" IN 3 MONTHS, ALMOST ALL USERS AFFECTED


- A seller showed that he was in possession of 700 million LinkedIn user records. That means almost all (92 percent) of LinkedIn's users are affected by this.
- The seller confirmed that they abused LinkedIn's API to scrape data. And sells them for \$5,000 USD.
- The records include full names, gender, email addresses, phone numbers and industry information.



CYBER ATTACKS



FAKE APPS TARGETING VACCINE REGISTRATION PROGRAMMES IN INDIA

- McAfee's latest Mobile Threat Report finds hackers capitalising on the pandemic to target unsuspecting consumers.
- These include fake apps targeting vaccine registration programmes and India and Chile have been most attacked with these campaigns. They also include billing fraud malware that makes purchases behind the backs of consumers. Hackers are also using banking Trojans to target hundreds of financial institutions around the world. 



RSS NEWSREADER NEWSBLUR TAKEDOWN

- RSS newsreader NewsBlur Takedown company's MongoDB database had been deleted and demanding a BTC 0.03 ransom (around \$1,000) for the recovery of 250 GB of data.
- Process had circumvented some firewall rules and left the NewsBlur MongoDB database unprotected.



Malware and Vulnerabilities



Adobe Experience Manager

ZERO-DAY EXPLOIT FOUND IN ADOBE EXPERIENCE MANAGER

- A zero-day vulnerability has been discovered in a popular content management solution used by high-profile companies.
- If the bug is left unchecked, the weakness allows attackers to bypass authentication and gain access to CRX Package Manager, leaving applications open to remote code execution (RCE) attacks. [↗](#)



MICROSOFT DISCLOSES CRITICAL BUGS ALLOWING TAKEOVER OF NETGEAR ROUTERS

- Cybersecurity researchers have detailed critical security vulnerabilities affecting NETGEAR DGN2200v1 series routers, which they say could be reliably abused as a jumping-off point to compromise a network's security and gain unfettered access.
- The flaws allow accessing router management pages using an authentication bypass, enabling an attacker to gain complete control over the router, as well ...



MICROSOFT ADMITS TO SIGNING ROOTKIT MALWARE IN SUPPLY-CHAIN FIASCO

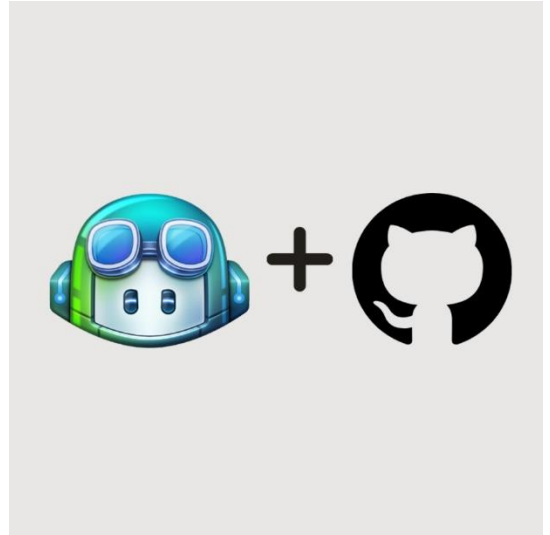
- Microsoft has now confirmed signing a malicious driver being distributed within gaming environments. This driver, called "Netfilter," is in fact a rootkit that was observed communicating with Chinese command-and-control (C2) IPs.
- Microsoft is actively investigating this incident, although thus far, there is no evidence that stolen code-signing certificates were used. [↗](#)

PRINTNIGHTMARE RCE FROM MICROSOFT

- PrintNightware, a critical Windows print spooler vulnerability that allowed for remote code execution was known as CVE-2021-1675.
- A remote code execution vulnerability exists when the Windows Print Spooler service improperly performs privileged file operations. [↗](#)

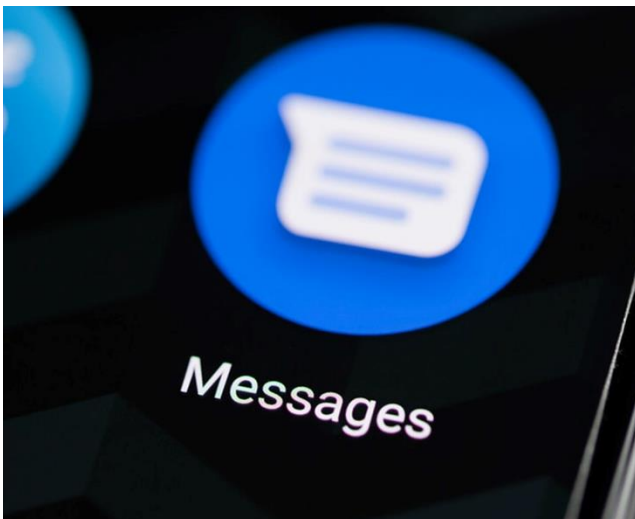


CYBER TECH



GOOGLE E2EE FOR ANDROID MESSAGE APP


- Google announced end-to-end encryption is now available in Android, but only for one-on-one conversations between users of the Messages app.
- The encryption feature has been available for beta testers since late 2020 but is now being rolled into the Android operating system for all users with chat features enabled.



GITHUB LAUNCHES 'COPILOT' — AI- POWERED CODE COMPLETION TOOL

- GitHub on Tuesday launched a technical preview of a new AI-powered pair programming tool that aims to help software developers write better code across a variety of programming languages, including Python, JavaScript, TypeScript, Ruby, and Go.
- Copilot, has been developed in collaboration with OpenAI, and leverages Codex, a new AI system that's trained on publicly available source code and natural language with the goal of translating comments and code written by a user into auto-generated code snippets. 

WINDOWS 11 WILL LET YOU RUN ANDROID APPS DIRECTLY ON THE DESKTOP

- During Windows 11 event, Microsoft announced that Android apps are coming to Windows 11 and can be run just like any other application installed in the operating system.
- Microsoft has partnered with the Amazon Appstore to quickly bring Windows 11 users an extensive catalogue of Android apps. This partnership will allow Windows 11 users access to games and a wide assortment of utilities and productivity apps. 



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.

MANAGED SECURITY SERVICES



Cybersecurity Monitoring and Management Services

There is a global need for expertise in managing complex IT Security Infrastructures. Infopercept provides IT Security and Infrastructure services as a Managed Security Service Provider (MSSP) and is a leading contributor in this segment. Infopercept delivers Managed Security Services globally in line with industry leading security policies, frameworks and technologies. We are powered by an inhouse team of highly competent cybersecurity professionals with vast practical exposure. Our practices have been developed over the years to protect client interests and fulfill their needs.



SECURE • OPTIMIZE • STRENGTHEN

+91 98988 57117

sos@infopercept.com

www.infopercept.com

