NIC IN NEWS

Date: 04-11-2019

N1. No harm in heirs of leaders entering politics, says Stalin

Times of India-Nov. 04 , 2019

From June this year, Tamil Nadu traffic police has been issuing payment challan developed by **National Informatics Centre**. While the receipt was printed only in ...

News Source: https://timesofindia.indiatimes.com/city/trichy/no-harm-in-heirs-of-leaders-entering-politics-says-stalin/articleshowprint/71882636.cms

N2. Priyanka Gandhi was warned by WhatsApp, says Congress

The Hindu-Nov 03 , 2019

... the Congress said telephone and internet providers for the government including the MTNL, National Internet Backbone and **National Informatics Centre** were ...

News Source: https://www.thehindu.com/news/national/whatsapp-alerted-priyanka-gandhi-vadra-on-possible-phone-attack-says-congress/article29870688.ece

N3. Only Hindi and English; Tamil missing in traffic challans in state

Times of India-Nov. 02 , 2019

Chennai: In June, more than two months before Union home minister Amith Shah sparked a controversy by saying Hindi should be the national language, traffic ...

News Source: https://timesofindia.indiatimes.com/city/chennai/only-hindi-and-english-tamil-missing-in-traffic-challans-in-state/articleshowprint/71872618.cms

N4. Delhi HC Raps Trade Marks Registry For Delay In Registrations, Says Process Needs to Be Streamlined

Live Law-Nov. 01 , 2019

The court also directed technical person from the **National Informatics Centre** and a senior officer from the Trade Mark Registry, Delhi who is familiar with the ...

News Source:https://www.livelaw.in/news-updates/delhi-hc-raps-trade-marks-registry-for-delay-in-registrations-149410

N5. Owners of property registered since 1986, beware! You are under watch

The New Indian Express-Nov. 01 , 2019

“The **National Informatics Centre** (NIC) is developing an online system in which officers would record details of offenders. The system would be ready in two ...

News Source: http://www.newindianexpress.com/states/kerala/2019/nov/02/owners-of-property-registered-since-1986-beware-you-are-under-watch-2055881.html

M1. WhatsApp snooping: IT ministry may seek more clarifications from social media giant

Financial Express-Nov. 04 , 2019

The Ministry of **electronics and IT** (MeitY) is likely to seek more clarifications from WhatsApp regarding the snooping attack as it studies the reply submitted by the ...

News Source: https://www.financialexpress.com/india-news/whatsapp-snooping-it-ministry-may-seek-more-clarifications-from-social-media-giant/1753451/

M2. Gulshan Rai: 'Govt is trying its best to protect but WhatsApp should've stopped the breach'

The Indian Express-Nov. 04 , 2019

Gulshan Rai was the National **Cybersecurity** Coordinator in the Prime .... People are alleging the Government of **India** (is involved) but there is no evidence.

News Source: https://indianexpress.com/article/india/gulshan-rai-govt-is-trying-its-best-to-protect-but-whatsapp-shouldve-stopped-the-breach-6101514/

M3. Where did the advisory note go: Experts quiz CERT-In

Economic Times – Nov. 04 , 2019

On the missing web page note, CERTIn had provided a detailed explanation of the vulnerability, which could be exploited by an attacker by making a decoy voice call to a target. It had warned WhatsApp users that the vulnerability could allow an attacker to access information on the system.

BENGALURU: Cyber law experts have asked the government to explain why the Indian computer emergency response team (CERT-In) removed from its website two days ago an advisory it had put out in May warning users of a vulnerability that could be used to exploit WhatsApp on their smartphones.

“This is merely further evidence that the explanation is to be provided by GoI (Government of India) instead of blame shifting and politicising the issue,” said Mishi Choudhary, the legal director of the New York-based Software Freedom Law Center. “India is a surveillance state with no judicial oversight.”

The development was first reported by The Times of India. On the missing web page note, CERTIn had provided a detailed explanation of the vulnerability, which could be exploited by an attacker by making a decoy voice call to a target.

It had warned WhatsApp users that the vulnerability could allow an attacker to access information on the system, such as logs, messages and photos, and could further compromise it.

CERT-In rated the severity “high” and asked users to upgrade to the latest version of the app. It also listed links to hackernews and cyber security firm Check Point Software that pointed to the alleged involvement of Israeli cyber software firm NSO Group in the hacking of WhatsApp messenger.

News Source: https://ciso.economictimes.indiatimes.com/news/where-did-the-advisory-note-go-experts-quiz-cert-in/71884394