China's New Law Requires Vendors to Report Zero-Day Bugs to Government

The Hacker News ⋮ 2-3 minutes

The Cyberspace Administration of China (CAC) has issued new stricter vulnerability disclosure regulations that mandate software and networking vendors affected with critical flaws to mandatorily disclose them first-hand to the government authorities within two days of filing a report.

The "Regulations on the Management of Network Product Security Vulnerability" are expected to go into effect starting September 1, 2021, and aim to standardize the discovery, reporting, repair, and release of security vulnerabilities and prevent security risks.

"No organization or individual may take advantage of network product security vulnerabilities to engage in activities that endanger network security, and shall not illegally collect, sell or publish information on network product security vulnerabilities," Article 4 of the regulation states.

In addition to banning sales of previously unknown security weaknesses, the new rules also forbid vulnerabilities from being disclosed to "overseas organizations or individuals" other than the products' manufacturers, while noting that the public disclosures should be simultaneously accompanied by the release of repairs or preventive measures.

"It is not allowed to deliberately exaggerate the harm and risk of network product security vulnerabilities, and shall not use network product security vulnerability information to carry out malicious speculation or fraud, extortion and other illegal and criminal activities," Article 9 (3) of the regulation reads.

Furthermore, it also prohibits the publication of programs and tools to exploit vulnerabilities and put networks at a security risk.

Found this article interesting? Follow us on Twitter and LinkedIn to read more exclusive content we post.