Newly found online security flaw stems from 1990s

March 4 2015, by Rob Lever

A newly discovered Internet security flaw could leave many websites vulnerable to hackers because of weak US encryption standards in the 1990s, researchers said Tuesday

A newly discovered Internet security flaw could leave many websites vulnerable to hackers because of weak US encryption standards in the 1990s, researchers said Tuesday.

The flaw dubbed "FREAK" could leave thousands of websites open to

attacks if the problem is not patched, according to papers released by French and US researchers.

The flaw was discovered by a team led by Karthikeyan Bhargavan at INRIA in Paris—the French Institute for Research in Computer Science and Automation—and disclosure coordinated by Matthew Green, a cryptographer at Johns Hopkins University.

A research paper said the flaw comes from "a class of deliberately weak export cipher suites... introduced under the pressure of US government agencies to ensure that the NSA would be able to decrypt all foreign encrypted communication."

Green said in a blog post that even some sites maintained by the National Security Agency and FBI appeared to be vulnerable.

"Since the NSA was the organization that demanded export-grade crypto, it's only fitting that they should be the first site affected by this vulnerability," Green said.

Green and other researchers said the flaw stems from US government-imposed standards for encryption in software that was exported—a short-lived effort to allow the United States to be able to access software exported to unfriendly regimes.

Part of the software

Even after it became legal to export strong encryption, the export mode feature was not removed from because some software still depended on it, according to Ed Felten, a Princeton University computer science professor.

"The flaw is significant in itself, but it is also a good example of what

can go wrong when government asks to build weaknesses into security systems," said Felten in a blog post.

"Many web sites are vulnerable to this attack, allowing an adversary in the network to spoof or spy on traffic to vulnerable sites."

Felten said that the vulnerability on the NSA site is "not a big national security problem in itself because NSA doesn't distribute state secrets from its public site. But there is an important lesson here about the consequences of crypto policy decisions."

Green said Facebook's site which operates the "like" button was identified as vulnerable but later patched.

Green said the most of the flaws "will soon be patched" but that the flaw is important at a time when the NSA is seeking to maintain access to encrypted software and devices for national security reasons.

"The moral of this story is pretty simple: Encryption backdoors will always turn around and bite you in the ass," he wrote.

Citation: Newly found online security flaw stems from 1990s (2015, March 4) retrieved 14 May 2024 from https://phys.org/news/2015-03-newly-online-flaw-stems-1990s.html