

The Internet goes on high alert after discovery of 8 compromised TLS certs

Security personnel around the world are on high alert Tuesday following the discovery of eight TLS certificates with private keys so weak they could allow anyone to mint trusted browser and app credentials for any site on the Internet.

As of late morning Tuesday, browser makers and some major apps and programming languages had blocked all eight of the intermediate certificates. There are no reports of certificate transparency logs, which track the issuance of all browser-trusted certificates, showing the compromised keys being used maliciously. The threat remains far from over, however, because it will be hard and time-consuming to update other key parts of the Internet, such as Linux distributions and embedded and Internet of Things devices.

One word: bonkers

The eight intermediate certificates belong to India-based certificate authority eMudhra Limited. An informal advisory published to emudhra.we-have-a-problem.com over on Tuesday posted the message “We have a problem here – Wayne.” The words were digitally signed using the private key of one of the eMudhra certificates. With proof that the reporting party had control of the key, defenders scrambled because the same key could be used to sign unauthorized certificates that would be trusted by millions of servers worldwide.

[Read full article](#)

[Comments](#)

<https://arstechnica.com/security/2026/10/the-internet-goes-on-high-alert-after-discovery-of-8-compromised-tls-certs/>