4 Social App does not validate server certificates for outgoing connections

Share:

TIMELINE

sanktjodel submitted a report to **Nextcloud**. Jul 4th (2 years ago)

The Social App (https://apps.nextcloud.com/apps/social) does not validate the server TLS certificate for connections to other ActivityPub servers.
These connections are used to retrieve the public key for a user or posting a message to another ActivityPub server.
The public key for a user is used to validate the ActivityPub user.

The vulnerable code is at https://github.com/daita/my-small-php-tools/blob/d8778803612af20699c7efb0637bfe62478e596c/lib/Traits/TRequest.php#L151.
The initRequest method disables verifying of the peer's certificate by setting CURLOPT_SSL_VERIFYPEER to FALSE.
This code is called from CurlService.php
(https://github.com/nextcloud/social/blob/97fb063479d4c0ad6fccdea3774601a619f8a886/lib/Service/CurlService.php#L265).

This issue has been tested on Nextcloud version version 19.0.0.12 with Social version 0.3.1.

Impact

An attacker can perform a man-in-the-middle attack by impersonating the victim server by using a self-signed TLS certificate.
The attacker would have to be in a privileged network position between the Nextcloud instance and the target ActivityPub server.