SmartAsset-CORS-CVE-2020-26527

CVE-2020-26527

Smart Asset - version 2020.7

An issue was discovered in API/api/Version in Damstra Smart Asset 2020.7. Cross-origin resource sharing trusts random origins by accepting the arbitrary 'Origin: example.com' header and responding with 200 OK and a wildcard 'Access-Control-Allow-Origin: *' header.

HTTP Request:

GET /API/api/Version HTTP/1.1 Origin: https://StudniarzLukasz.com <---------- Cookie: _ga=GA1.3.1950130407.1600387365; _gid=GA1.3.1208628208.1600387365; _gat_gtag_UA_100469070_4=1; ajs_group_id=null; intercom-id-zk1ecu97=47f0bf3f-35aa-4f97-9239-456a2678da65; intercom-session-zk1ecu97=

HTTP Response:

HTTP/1.1 200 OK Access-Control-Allow-Origin: * <---------- Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept, Authorization Strict-Transport-Security: max-age=31536000; includeSubDomains

{"Version":"2020.5 (Build 36 Revision 40954)","AssemblyVersion":"20.5.36.40954","BuildDate":"2020-07-27T13:21:18+10:00","CompanyName":"SmartAsset Software","LegalCopyright":"Copyright .. SmartAsset <>

[Discoverer] Lukasz Studniarz