


43

CORS Misconfiguration leading to Private Information Disclosure

Share:      

State  Resolved (Closed)


Disclosed **June 7, 2019 2:01pm +0200**



Reported To [Ubiquiti Networks](#)

Asset *.ubnt.com
(Domain)

Weakness Improper Access Control - Generic

Bounty \$500

Severity  High (7 ~ 8.9)

Participants  

Visibility Disclosed (Limited)

Collapse

SUMMARY BY UBIQUITI NETWORKS






Due to mistake on te CORS policy configuration, the sites <https://client.amplifi.com> and <https://protect.ubnt.com/> CORS policy allowed HTTP requests to be made from certain sites outside the *.ubnt.com and *.ui.com domains.

This bug could be used to steal users information or force the user to execute unwanted actions. As long that a legit and logged in user is lure to access a attacker controlled HTML page.

TIMELINE · EXPORT



- [sandh0t](#) submitted a report to [Ubiquiti Networks](#). Oct 29th (9 months ago)
- [sandh0t](#) posted a comment. Oct 30th (9 months ago)
- [ubnt-rubens](#) changed the status to  Triaged. Oct 31st (9 months ago)
- [sandh0t](#) posted a comment. Oct 31st (9 months ago)
- [sandh0t](#) posted a comment. Nov 6th (9 months ago)
- [sandh0t](#) posted a comment. Nov 13th (9 months ago)
- [sandh0t](#) posted a comment. Nov 16th (8 months ago)
- [ubnt-rubens](#) posted a comment. Nov 16th (8 months ago)
- [sandh0t](#) posted a comment. Nov 19th (8 months ago)
- [sandh0t](#) posted a comment. Nov 23rd (8 months ago)
- [Ubiquiti Networks](#) rewarded [sandh0t](#) with a \$500 bounty. Nov 26th (8 months ago)
- [ubnt-rubens](#) closed the report and changed the status to  Resolved. Nov 26th (8 months ago)
- [sandh0t](#) requested to disclose this report. May 13th (3 months ago)
- [ubnt-rubens](#) agreed to disclose this report. Jun 7th (2 months ago)

 This report has been disclosed.

Jun 7th (2 months ago)