



CVE-2020-9449

Published on: 02/28/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:13 PM UTC

CVE-2020-9449

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Blab! Ax](#) from [Justblab](#) contain the following vulnerability:

An insecure random number generation vulnerability in BlaB! AX, BlaB! AX Pro, BlaB! WS (client), and BlaB! WS Pro (client) version 19.11 allows an attacker (with a guest or user session cookie) to escalate privileges by retrieving the cookie salt value and creating a valid session cookie for an arbitrary user or admin.

CVE-2020-9449 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector

Attack Complexity

Privileges Required

User Interaction

NETWORK

LOW

LOW

NONE

Scope

Confidentiality Impact

Integrity Impact

Availability Impact

UNCHANGED

HIGH

HIGH

HIGH

CVSS2 Score: **6.5 - MEDIUM**

Access Vector

Access Complexity

Authentication

NETWORK

LOW

SINGLE

Confidentiality Impact

Integrity Impact

Availability Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

News!

[Vendor Advisory](#)
[justblab.com](#)
[text/html](#)

[B](#) MISC [justblab.com/latest-news](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Justblab	Blab! Ax	19.11	All	All	All
Application	Justblab	Blab! Ax	19.11	All	All	All
Application	Justblab	Blab! Ax Pro	19.11	All	All	All
Application	Justblab	Blab! Ax Pro	19.11	All	All	All
Application	Justblab	Blab! Ws	19.11	All	All	All
Application	Justblab	Blab! Ws	19.11	All	All	All
Application	Justblab	Blab! Ws Pro	19.11	All	All	All
Application	Justblab	Blab! Ws Pro	19.11	All	All	All
cpe:2.3:a:justblab:blab\!_ax:19.11:****:****:						
cpe:2.3:a:justblab:blab\!_ax:19.11:****:****:						
cpe:2.3:a:justblab:blab\!_ax_pro:19.11:****:****:						
cpe:2.3:a:justblab:blab\!_ax_pro:19.11:****:****:						
cpe:2.3:a:justblab:blab\!_ws:19.11:****:****:						
cpe:2.3:a:justblab:blab\!_ws:19.11:****:****:						
cpe:2.3:a:justblab:blab\!_ws_pro:19.11:****:****:						
cpe:2.3:a:justblab:blab\!_ws_pro:19.11:****:****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

