



CVE-2020-21989

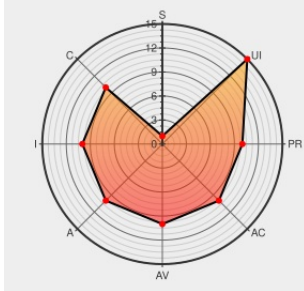
Published on: 04/27/2021 12:00:00 AM UTC

Last Modified on: 05/06/2021 02:05:00 PM UTC

CVE-2020-21989

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

CVSS:31/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



Certain versions of [Homeautomation](#) from [Homeautomation Project](#) contain the following vulnerability:

HomeAutomation 3.3.2 is affected by Cross Site Request Forgery (CSRF). The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web

site.

CVE-2020-21989 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	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Zero Science Lab » HomeAutomation v3.3.2 CSRF Add Admin Exploit	www.zeroscience.mk text/html	MISC www.zeroscience.mk/en/vulnerabilities/ZSL-

HomeAutomation 3.3.2 - Cross-Site Request Forgery (Add Admin) - PHP webapps Exploit

[www.exploit-db.com](#)
[Proof of Concept](#)
[text/html](#)

 [EXPLOIT-DB Exploit Database](#)

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	Homeautomation Project	Homeautomation	3.3.2	All	All	All
cpe:2.3:a:homeautomation_project:homeautomation:3.3.2:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2020-21989 : HomeAutomation 3.3.2 is affected by Cross Site Request Forgery CSRF . The application interface a... twitter.com/i/web/status/1...	2021-04-27 18:07:17
 /r/netcve	CVE-2020-21989	2021-04-27 18:41:37

[← Previous ID](#)

[Next ID →](#)