



CVE-2020-22001

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-22001
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-27 18:15:00 UTC
Updated	2022-10-26 13:59:00 UTC
Description	HomeAutomation 3.3.2 suffers from an authentication bypass vulnerability when spoofing client IP address using the X-For

Risk And Classification

Problem Types: CWE-290

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Homeautomation Project	Homeautomation	3.3.2	All	All	All

References

Reference	Source	Link	Tags
Zero Science Lab » HomeAutomation v3.3.2 Authentication Bypass Exploit	MISC	www.zeroscience.mk	
HomeAutomation 3.3.2 - Authentication Bypass - PHP webapps Exploit	EXPLOIT-DB	www.exploit-db.com	
CWE - CWE-290: Authentication Bypass by Spoofing (4.3)	MISC	cwe.mitre.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report