



# CVE-2020-22000

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

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

## CVE-2020-22000

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

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

HomeAutomation 3.3.2 suffers from an authenticated OS command execution vulnerability using custom command v0.1 plugin. This can be exploited with a CSRF vulnerability to execute arbitrary shell commands as the web user via the 'set\_command\_on' and 'set\_command\_off' POST parameters in

'/system/systemplugins/customcommand/customcommand.plugin.php' by using an unsanitized PHP exec() function.

CVE-2020-22000 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>LOW</b>          | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **8.5 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>SINGLE</b>       |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>COMPLETE</b>        | <b>COMPLETE</b>   | <b>COMPLETE</b>     |

## CVE References

| Description                                                  | Tags                           | Link                                        |
|--------------------------------------------------------------|--------------------------------|---------------------------------------------|
| HomeAutomation 3.3.2 - Remote Code Execution - PHP webserver | <a href="#">CVE-2020-22000</a> | <a href="#">EXPLOIT-DB Exploit Database</a> |

HomeAutomation 3.3.2 - Remote Code Execution - PHP webapps Exploit

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

Zero Science Lab » HomeAutomation v3.3.2 CSRF Remote Command Execution (PHP Reverse Shell) PoC

[www.zeroscience.mk](#)[text/html](#)

MISC[www.zeroscience.mk/en/vulnerabilities/ZSL-2019-5560.php](#)

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](mailto: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 | <a href="#">Homeautomation Project</a> | <a href="#">Homeautomation</a> | 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-2020-22000 : HomeAutomation 3.3.2 suffers from an authenticated OS command execution vulnerability using custom... <a href="#">twitter.com/i/web/status/1...</a> | 2021-04-27 18:08:08 |
| /r/netcve  | <a href="#">CVE-2020-22000</a>                                                                                                                                       | 2021-04-27 18:41:39 |

← Previous ID

Next ID→