



CVE-2021-20991

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

Summary

CVE	CVE-2021-20991
State	PUBLIC
Assigner	info@cert.vde.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-19 14:15:00 UTC
Updated	2022-04-26 16:03:00 UTC
Description	In Fibaro Home Center 2 and Lite devices with firmware version 4.540 and older an authenticated user can run commands

Risk And Classification

Problem Types: CWE-77

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Fibaro	Home Center 2	-	All	All	All
Operating System	Fibaro	Home Center 2 Firmware	All	All	All	All
Hardware	Fibaro	Home Center Lite	-	All	All	All
Operating System	Fibaro	Home Center Lite Firmware	All	All	All	All

References

Reference	S
Advisory: Multiple Vulnerabilities in Fibaro Home Center - IoT Inspector	C
Fibaro Home Center MITM / Missing Authentication / Code Execution ≈ Packet Storm	M
Full Disclosure: [CVE-2021-20989, CVE-2021-20990, CVE-2021-20991, CVE-2021-20992] Multiple vulnerabilities in Fibaro Home Center	F
CVE Program record	C
NVD vulnerability detail	N

Vendor Comments And Credit

Discovery Credit

LEGACY: Marton Illes IoT Inspector Research Lab <https://www.iot-inspector.com>

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)