



CVE-2022-47189

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

Summary

CVE	CVE-2022-47189
State	PUBLIC
Assigner	cve-coordination@incibe.es
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-31 22:15:00 UTC
Updated	2023-04-06 20:12:00 UTC
Description	Generex UPS CS141 below 2.06 version, allows an attacker to upload a firmware file containing an incorrect configuration, i

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Generex	Cs141	-	All	All	All
Operating System	Generex	Cs141 Firmware	All	All	All	All

References

Reference	Source	Link	Tags
BACS, CS141, SITEMANAGER and SITEMONITOR Firmware Generex	CONFIRM	www.generex.de	
[Update 03/03/2023] Multiple vulnerabilities in Generex UPS CS141 INCIBE-CERT	CONFIRM	www.incibe-cert.es	
2.12 Generex	CONFIRM	www.generex.de	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Joel Gámez Molina (@JoelGMSec)

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](#).

Free CVE JSON API [cve.report/api](#)

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