



CVE-2022-33202

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

Summary

CVE	CVE-2022-33202
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-27 01:15:00 UTC
Updated	2022-07-07 14:07:00 UTC
Description	Authentication bypass vulnerability in the setup screen of L2Blocker(on-premise) Ver4.8.5 and earlier and L2Blocker(Cloud)

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Softcreate	L2blocker	All	All	All	All
Application	Softcreate	L2blocker	All	All	All	All

References

Reference	Source	Link	Tags
L2Blockerセンサー設定画面における、認証回避の脆弱性 株式会社ソフトクリエイト	MISC	www.softcreate.co.jp	
JVN#51464799: L2Blocker Sensor setup screen vulnerable to authentication bypass	MISC	jvn.jp	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

No vendor comments have been submitted for this CVE.

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

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