CVE-2022-22110

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-22110
State	PUBLIC
Assigner	vulnerabilitylab@whitesourcesoftware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-05 15:15:00 UTC
Updated	2022-01-21 14:24:00 UTC
Description	In Daybyday CRM, versions 1.1 through 2.2.0 enforce weak password requirements in the user update functionality. A user

Risk And Classification

Problem Types: CWE-521

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Daybydaycrm	Daybyday Crm	All	All	All	All

References

Reference	Source	Link
password change requires 6 on update, and only allowed users can see … · Bottelet/DaybydayCRM@a0392f4 · GitHub	CONFIRM	github
CVE-2022-22110 | WhiteSource Vulnerability Database	MISC	www.
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

Vendor Comments And Credit

Discovery Credit

LEGACY: WhiteSource Vulnerability Research Team (WVR)

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

Free CVE JSON API cve.report/api

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