CVE-2020-14011

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

Summary

CVE	CVE-2020-14011
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-15 15:15:00 UTC
Updated	2022-04-26 18:56:00 UTC
Description	Lansweeper 6.0.x through 7.2.x has a default installation in which the admin password is configured for the admin account,

Risk And Classification

Problem Types: CWE-1188

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lansweeper	Lansweeper	All	All	All	All

References

Reference	Source	Link	Tags
Pastebin.com - Not Found (#404)	MISC	pastebin.com	Third Party Advisory
Restrict access to the web console | Lansweeper | IT Discovery Software	MISC	www.lansweeper.com	Vendor Advisory
Lansweeper 7.2 Default Account / Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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