CVE-2020-7356

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

Summary

CVE	CVE-2020-7356
State	PUBLIC
Assigner	cve@rapid7.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-08-06 16:15:00 UTC
Updated	2020-08-12 13:39:00 UTC
Description	CAYIN xPost suffers from an unauthenticated SQL Injection vulnerability. Input passed via the GET parameter 'wayfinder_s

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cayintech	Xpost	1.0	All	All	All
Application	Cayintech	Xpost	2.0	All	All	All
Application	Cayintech	Xpost	2.5.18103	All	All	All
Application	Cayintech	Xpost	1.0	All	All	All
Application	Cayintech	Xpost	2.0	All	All	All
Application	Cayintech	Xpost	2.5.18103	All	All	All

References

Reference	Source	Link
Cayin xPost and CMS exploits by h00die · Pull Request #13607 · rapid7/metasploit-framework · GitHub	MISC	github.com
Zero Science Lab » Cayin Digital Signage System xPost 2.5 Pre-Auth SQLi Remote Code Execution	MISC	www.zeroscience.mk
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: This issue was discovered by Gjoko Krstic of Zero Science Lab.

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