



CVE-2022-30245

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

Summary

CVE	CVE-2022-30245
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-15 12:15:00 UTC
Updated	2022-07-25 17:50:00 UTC
Description	Honeywell Alerton Compass Software 1.6.5 allows unauthenticated configuration changes from remote users. This enables

Risk And Classification

Problem Types: CWE-610

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Honeywell	Alerton Compass	1.6.5	All	All	All

References

Reference	Source
SCADAfence Blog	MISC
Product Security	MISC
GitHub - scadafence/Honeywell-Alerton-Vulnerabilities: Alerton Ascent Control Module (ACM) & Alerton Visual Logic vulnerabilities	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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