CVE-2018-19783

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

Summary

CVE	CVE-2018-19783
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-21 16:00:00 UTC
Updated	2019-03-27 17:26:00 UTC
Description	Kentix MultiSensor-LAN 5.63.00 devices and previous allow Authentication Bypass via an Alternate Path or Channel.

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Kentix	Multisensor-lan	-	All	All	All
Hardware	Kentix	Multisensor-lan	-	All	All	All
Operating System	Kentix	Multisensor-lan Firmware	All	All	All	All

References

Reference	Source	Link	Ta
Kentix MultiSensor-LAN 5.63.00 Authentication Bypass ≈ Packet Storm	MISC	packetstormsecurity.com	Ex
Bugtraq: [SYSS-2018-043] Authentication Bypass in Kentix MultiSensor LAN - CVE-2018-19783	MISC	seclists.org	Ex
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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