CVE-2016-9347

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

Summary

CVE	CVE-2016-9347
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-13 21:59:00 UTC
Updated	2017-03-13 16:52:00 UTC
Description	An issue was discovered in Emerson SE4801T0X Redundant Wireless I/O Card V13.3, and SE4801T1X Simplex Wireless

Risk And Classification

Problem Types: CWE-254

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Emerson	Se4801t0x Redundant Wireless I/o Card	-	All	All	All
Operating System	Emerson	Se4801t0x Redundant Wireless I/o Card Firmware	13.3	All	All	All
Hardware	Emerson	Se4801t0x Redundant Wireless I/o Card	-	All	All	All
Hardware	Emerson	Se4801t0x Redundant Wireless I/o Card	-	All	All	All
Operating System	Emerson	Se4801t0x Redundant Wireless I/o Card Firmware	13.3	All	All	All
Operating System	Emerson	Se4801t0x Redundant Wireless I/o Card Firmware	13.3	All	All	All
Hardware	Emerson	Se4801t1x Simplex Wireless I/o Card	-	All	All	All
Operating System	Emerson	Se4801t1x Simplex Wireless I/o Card Firmware	13.3	All	All	All
Hardware	Emerson	Se4801t1x Simplex Wireless I/o Card	-	All	All	All
Hardware	Emerson	Se4801t1x Simplex Wireless I/o Card	-	All	All	All
Operating System	Emerson	Se4801t1x Simplex Wireless I/o Card Firmware	13.3	All	All	All
Operating System	Emerson	Se4801t1x Simplex Wireless I/o Card Firmware	13.3	All	All	All

References

Reference	Source	Link	Tags
Emerson DeltaV Wireless I/O Card Open SSH Port Vulnerability | ICS-CERT	MISC	ics-cert.us-cert.gov	Third Party Advisory, U
Multiple Emerson Products CVE-2016-9347 Security Bypass Vulnerability	BID	www.securityfocus.com	Third Party Advisory, V

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.

Legacy QID Mappings

590585 Emerson DeltaV Wireless I/O Card Open SSH Port Vulnerability (ICSA-16-334-03)

Free CVE JSON API cve.report/api

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