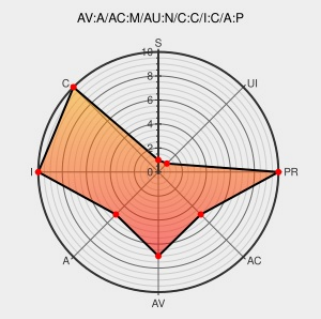
# CVE-2014-2378

Published on: 09/05/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:58 PM UTC

## CVE-2014-2378

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Trafficdot from Sensysnetworks contain the following vulnerability:

Sensys Networks VSN240-F and VSN240-T sensors VDS before 2.10.1 and TrafficDOT before 2.10.3 do not verify the integrity of downloaded updates, which allows remote attackers to execute arbitrary code via a Trojan horse update.

CVE-2014-2378 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability

### CVSS2 Score: 7.6 - HIGH

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| ADJACENT_NETWORK | MEDIUM | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| COMPLETE | COMPLETE | PARTIAL |

### CVE References

| Description | Tags | Link |
|---|---|---|
| Sensys Networks Traffic Sensor Vulnerabilities (Update A) \| ICS-CERT | US Government Resource, web.archive.org, text/html, Inactive Link, Not Archived | MISC ics-cert.us-cert.gov/advisories/ICSA-14-247-01 |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

### Known Affected Configurations (CPE V2.3)

Known Affected Configurations (CPE v2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Sensysnetworks | Trafficdot | 2.10.0 | All | All | All |
| Application | Sensysnetworks | Trafficdot | 2.10.1 | All | All | All |
| Application | Sensysnetworks | Trafficdot | 2.8.3 | All | All | All |
| Application | Sensysnetworks | Trafficdot | 2.10.0 | All | All | All |
| Application | Sensysnetworks | Trafficdot | 2.10.1 | All | All | All |
| Application | Sensysnetworks | Trafficdot | 2.8.3 | All | All | All |
| Application | Sensysnetworks | Trafficdot | All | All | All | All |
| Application | Sensysnetworks | Vds | 1.8.5 | All | All | All |
| Application | Sensysnetworks | Vds | 1.8.7 | All | All | All |
| Application | Sensysnetworks | Vds | 2.6.3 | All | All | All |
| Application | Sensysnetworks | Vds | 2.6.4 | All | All | All |
| Application | Sensysnetworks | Vds | 1.8.5 | All | All | All |
| Application | Sensysnetworks | Vds | 1.8.7 | All | All | All |
| Application | Sensysnetworks | Vds | 2.6.3 | All | All | All |
| Application | Sensysnetworks | Vds | 2.6.4 | All | All | All |
| Application | Sensysnetworks | Vds | All | All | All | All |
| Hardware | Sensysnetworks | Vsn240-f | - | All | All | All |
| Hardware | Sensysnetworks | Vsn240-f | - | All | All | All |
| Hardware | Sensysnetworks | Vsn240-t | - | All | All | All |
| Hardware | Sensysnetworks | Vsn240-t | - | All | All | All |

cpe:2.3:a:sensysnetworks:trafficdot:2.10.0:*:*:*:*:*:*:*:

cpe:2.3:a:sensysnetworks:trafficdot:2.10.1:*:*:*:*:*:*:*:

cpe:2.3:a:sensysnetworks:trafficdot:2.8.3:*:*:*:*:*:*:*:

cpe:2.3:a:sensysnetworks:trafficdot:2.10.0:*:*:*:*:*:*:*:

cpe:2.3:a:sensysnetworks:trafficdot:2.10.1:*:*:*:*:*:*:*:

cpe:2.3:a:sensysnetworks:trafficdot:2.8.3:*:*:*:*:*:*:*:

cpe:2.3:a:sensysnetworks:trafficdot:*:*:*:*:*:*:*:*:

cpe:2.3:a:sensysnetworks:vds:1.8.5:*:*:*:*:*:*:*:

cpe:2.3:a:sensysnetworks:vds:1.8.7:*:*:*:*:*:*:*:

cpe:2.3:a:sensysnetworks:vds:2.6.3:*:*:*:*:*:*:*:

cpe:2.3:a:sensysnetworks:vds:2.6.4:*:*:*:*:*:*:*:

cpe:2.3:a:sensysnetworks:vds:1.8.5:*:*:*:*:*:*:*:

cpe:2.3:a:sensysnetworks:vds:1.8.7:*:*:*:*:*:*:*:

cpe:2.3:a:sensysnetworks:vds:2.6.3:*:*:*:*:*:*:*:

cpe:2.3:a:sensysnetworks:vds:2.6.4:*:*:*:*:*:*:*:

cpe:2.3:a:sensysnetworks:vds:*:*:*:*:*:*:*:*:

cpe:2.3:h:sensysnetworks:vsn240-f:-:*:*:*:*:*:*:*:

cpe:2.3:h:sensysnetworks:vsn240-f:-:*:*:*:*:*:*:*:

cpe:2.3:h:sensysnetworks:vsn240-t:-:*:*:*:*:*:*:*:

cpe:2.3:h:sensysnetworks:vsn240-t:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→